A Psychological Profile of Defender Personality Traits

Tara Whalen
Faculty of Computer Science, Dalhousie University, Halifax, NS, Canada
Email: whalen@cs.dal.ca

Carrie Gates*
CA Labs, CA Inc., Islandia, New York, USA
Email: carrie.gates@ca.com

Abstract— The security community has used psychological research on attacker personalities, but little work has been done to investigate the personalities of the defenders. One instrument currently dominating personality research is the Five Factor Model, a taxonomy that identifies five major domains of personal traits, composed of sets of facets. This model can be used within an organizational or vocational capacity to reveal dominant tendencies, such as openness to new experiences. Within a security context, this tool could show what patterns professionals exhibit, which may reveal areas of insufficient diversity and "blind spots" in defenses.

We surveyed 43 security professionals using a Five Factor Model-based test (the IPIP-NEO) to reveal common dominant traits. We found that our sampled security population demonstrated that they were highly dutiful, achievement-striving, and cautious; in addition, they were high in morality and cooperation, but low in imagination. We note that many of these characteristics seem to be appropriate for security professionals, although the low scores in the "openness to experience" domain may indicate difficulties in devising new security defense methods and in anticipating new forms of attack. This finding implies that security professionals might be more reactive to security threats, rather than proactive in discovering them before they are used by adversaries. This lack of anticipation could potentially leave large organizations vulnerable to attacks that might have otherwise been prevented.

I. INTRODUCTION

Within the security community, psychological research has traditionally been directed towards attackers: for example, the psychology underlying insider threats [36] or criminal hacker behavior [32]. However, another piece of the overall picture is the psychology of the *defender* who must guard against these threats. Security defenders respond to the approaches and actions taken by attackers: they develop counter-offensive strategies, and attempt to anticipate new threats. In a sense, attackers and defenders operate in an antagonistic partnership, considering the same sets of problems from different perspectives. Because psychology (specifically, personality traits) has been used to understand attackers, it is worth considering how their "partners", the defenders, might similarly be affected by psychological factors. Specifically, it is useful to understand how personality traits influence the effectiveness of security defenders. This in turn might indicate where there may be weaknesses in defence strategies.

There have been some recent steps in this direction. Greenwald *et al.* [14], in a panel on psychology in security, noted that profiling defenders might be "the most promising solution to the non-acceptance factor: a sensation-seeker is a risk taker, so he/she will not buy an InfoSec software package; if bought by somebody else, they will not install it; if forced to install, they will use the first customer complaint about a performance deficit as an excuse to uninstall it." These statements suggest that there are benefits to developing a better understanding of the personality aspects of security defenders.

In order to develop a more complete understanding of defender personality traits, we build upon an initial study that used the Myers-Briggs Type Indicator (MBTI) [11], and employed another current personality test: the Five Factor Model (FFM). This model has enjoyed recent favor within the psychology community, and has been widely adopted as a comprehensive testing instrument [26]. As opposed to the MBTI, which describes people in terms of one of 16 "types" of personalities, the FFM describes people in terms of five overall personality domains, each of which is further sub-divided into six traits ("facets").

We solicited the security professionals who attended the 2004 Annual Computer Security Applications Conference to complete the IPIP-NEO, a 120-item questionnaire based on the FFM. The results from this questionnaire were used to determine how the attendees compared to the general population on each of the five domains and 30 facets. We found that these professionals scored significantly higher on the domain conscientiousness and lower on the domain openness to new experience. This paper details the methodology and results from having this group of security professionals complete the Five Factor Model personality test.

Section II describes the Five Factor Model used as the basis of our investigation. Section III presents our experimental methodology and statistical results. Section IV discusses how the personality profiles may affect security practice. Section V presents some related work in this area. We describe future work in Section VI and conclude with some summary remarks in Section VII.

II. THE FIVE FACTOR MODEL

A. Overview of Five Factor Model

A dominant taxonomy within current personality research is the Five Factor Model (FFM), which uses five basic domains, each containing subfactors (or "facets") that make up that category. FFM uses the "OCEAN" domains: Openness to experience, Conscientiousness, Extraversion, Agreeableness, and Neuroticism [12]. A person will have different levels of each trait, which are compared to the rest of the population; for example, a person's test results may show that he is less extraverted than the average test subject, but more open to experience. The five FFM domains are described in detail below; the facets are from the International Personality Item Pool Representation of the NEO-PI-R (IPIP-NEO) [12], which was the FFM test used in this study.

Openness to Experience: this domain demonstrates a person's comfort with new ideas, abstractions, and imagination. The IPIP-NEO test characterizes Openness to Experience in the following way, "Open people are intellectually curious, appreciative of art, and sensitive to beauty. They tend to be, compared to closed people, more aware of their feelings. They tend to think and act in individualistic and nonconforming ways...Another characteristic of the open cognitive style is a facility for thinking in symbols and abstractions far removed from concrete experience" [19]. The facets of Openness are emotionality, artistic interests, imagination, adventurousness, liberalism, and intellect. (Note that intellect does not mean intelligence; rather, it refers to enjoyment of playing with ideas rather than with concrete people or things.)

Conscientiousness: this domain deals with impulse control and spontaneity. The IPIP-NEO states that "Impulses are not inherently bad; occasionally time constraints require a snap decision, and acting on our first impulse can be an effective response. Also, in times of play rather than work, acting spontaneously and impulsively can be fun...Nonetheless...Acting impulsively disallows contemplating alternative courses of action, some of which would have been wiser than the impulsive choice. Impulsivity also sidetracks people during projects that require organized sequences of steps or stages" [19]. The facets of Conscientiousness are self-efficacy, orderliness, dutifulness, achievement-striving, self-discipline, and cautiousness.

Extraversion: this domain describes the degree of engagement with the external world. According to IPIP-NEO "Extraverts enjoy being with people, are full of energy, and often experience positive emotions...In groups they like to talk, assert themselves, and draw attention to themselves. Introverts lack the exuberance, energy, and activity levels of extraverts. They tend to be quiet, low-key, deliberate, and disengaged from the social world" [19]. Introversion can sometimes be misinterpreted as depression or unfriendliness; however, introverts merely require less interaction with the social world, and may be quite agreeable and content. The facets of Extraversion are friendliness, gregariousness, assertiveness, activity level, excitement-seeking, and cheerfulness.

Agreeableness: this domain is focused on how much people value getting along with others. The IPIP-NEO states that "Agreeable individuals value getting along with others. They are therefore considerate, friendly, generous, helpful, and willing to compromise their interests with others'. Agreeable people also have an optimistic view of human nature. Disagreeable individuals place self-interest above getting along with others. They are generally unconcerned with others' well-being, and therefore are unlikely to extend themselves for other people" [19]. Agreeable people may be more popular, but disagreeableness can be an asset when making hard objective decisions. The facets of Agreeableness are trust, morality, altruism, cooperation, modesty, and sympathy. (Note that morality in this context does not refer to one's stance on issues of social significance, such as euthanasia, but rather indicate characteristics such as sincerity and lack of guardedness about telling the truth.)

Neuroticism: this domain has a somewhat misleading title, as it suggests the individual is suffering from Freudian neurosis. In current psychology parlance, neuroticism refers to a person's inclination to experience negative emotions (such as anxiety). According to the IPIP-NEO "People high in neuroticism are emotionally reactive. They respond emotionally to events that would not affect most people...These problems in emotional regulation can diminish a neurotic's ability to think clearly, make decisions, and cope effectively with stress...individuals who score low in neuroticism are less easily upset and are less emotionally reactive. They tend to be calm, emotionally stable, and free from persistent negative feelings" [19]. Note that those who are low on the neuroticism scale may not necessarily have positive emotions most of the time, merely a lack of frequent negative feelings. The facets of neuroticism are anxiety, anger, depression, self-consciousness, immoderation, and vulnerability.

B. Development of the Five Factor Model

The Five Factor Model is based on an analysis of the English language, rather than on the theory of any individual psychologist. Personality-related adjectives were extracted from a dictionary, and study participants were asked to use these adjectives to describe different people. Statistical correlations were used on the results to generate groups of adjectives that seemed to describe the same general trait. For example, adjectives such as "lively", "talkative" and "outgoing" were likely to be applied together, and thus represented the overall factor of extraversion. Fiske, in 1949, was the first to establish that there are five dominant factors in personality [9]. This was later confirmed and extended by Tupes and Christal [37]. Their work was in turn continued by Norman [28], who popularized the concept. After a hiatus of nearly 20 years, the idea of using five factors to characterize personalities

resurfaced in the early 1980s and has since been studied more extensively.

In this study we used the International Personality Item Pool (IPIP-NEO) online test, which was created by Goldberg in 1999 [12]. This test was designed to measure the same aspects as the NEO PI-R test (which is a similar, but proprietary, personality test using the "Big 5" as opposed to the Five Factor Model), as well as to be short enough to encourage subject completion. The IPIP researchers claim a high degree of correlation between the IPIP-NEO and the NEO PI-R test [12].

C. Scoring

A test subject who takes a Five Factor Model test (such as the IPIP-NEO) is presented with a series of questions to determine the level of a particular facet within each of the five domains. The score is based on a continuum, with subject scores falling along a normal distribution. Approximately half of the questions are keyed positively (towards the high end of the scale) and the other half, negatively; this provides some balance so that the responses are not biased toward one type of response.

Let us consider the example of one facet–sympathy–within the domain of Agreeableness. Some questions within the entire test would be designed to measure sympathy. Approximately half would be phrased positively ("Feel sympathy for those worse off than myself") and half negatively ("Am not interested in people's problems") [12]. Responses, in the IPIP 120-item test, are based on a 5-point Likert scale; the person can strongly agree, agree, be neutral, disagree or strongly disagree as to whether the statement describes them accurately [24]. The responses provide a level of sympathy, which can be compared to other test subjects, based on a normal distribution. We then see where the person falls in comparison to others, in terms of sympathy: less sympathetic, more sympathetic, or average. Sympathy can then be combined with other traits within the Agreeableness domain (such as morality and trust) to give an overall domain score, which again is located within a normal distribution. In summary, a person is evaluated in terms of an overall population, giving a comparative score expressed as a percentile.

III. METHOD

A. Sampling Procedure

We conducted a survey of security professionals in order to determine their personality characteristics using the NEO PI-R instrument [7]. This instrument is based on the Five Factor Model, which is widely accepted in mainstream personality psychology [26]. The other popular personality assessment device is the Myers-Briggs Type Indicator®(MBTI)[1], which assigns respondents to one of 16 personality "types". However, this tool is generally not as popular amongst psychologists [26]. We

[1]Myers-Briggs Type Indicator and MBTI are registered trademarks of Consulting Psychologists Press, Inc.

therefore chose the FFM, and concentrated on measuring personality traits as opposed to types.

The original NEO PI-R is copyrighted by Psychological Assessments Resources Inc. and is available for purchase by professionals [31], however we did not have the financial resources to use this particular test. In addition, this test has 240 questions and takes 35 to 45 minutes to complete. Given that our participants were all volunteers, we felt that they would be unwilling to invest that much time in completing the survey.

We therefore chose a related test, the IPIP (International Personality Item Pool) NEO [12] [18], which is similar to the NEO PI-R [7]. While the full IPIP test is in the public domain, it consists of 1,699 questions. Thus, we used a modified version of this test, developed by Dr. Johnson and available at `http://www.personal.psu.edu/faculty/j/5/j5j/IPIP/ipipneo120.htm`. This version consists of 120 questions about personality traits (*e.g.*, love large parties, prefer variety to routine), which subjects are asked to rate on a 5-point Likert scale from very inaccurate to very accurate. The answers are used to determine scores on 30 facets of personality, which are aggregated into five broad domains: neuroticism, extraversion, openness to experience, agreeableness and conscientiousness. This particular form of the IPIP NEO personality test uses the results from more than 20,000 respondents to ensure that it has an acceptable measurement reliability (according to `http://www.personal.psu.edu/faculty/j/5/j5j/IPIP/`).

The on-line questionnaire was converted to a paper format where subjects were asked to fill in the bubble for the response that most closely described them. The questionnaires were disseminated with the registration packets at the Annual Computer Security Applications Conference (ACSAC), held in December 2004. There were 177 attendees at this conference, 43 of whom returned completed survey questionnaires, providing a response rate of 24.3%. The attendees at this conference covered a broad spectrum of security professionals, including both researchers and practitioners from government, industry and academia.

B. Analysis

There were 43 responses to the survey: 31 men (72%), ten women (23%) and two people who did not provide their sex. (This is representative of the field in general, where the percentage of women employed in a computer/information science position in the United States is 26% [27].)

Of the 43 responses, we discarded the two who did not provide their sex, as well as an additional questionnaire where the true responses were difficult to determine. Of the remaining 40, only 23 responses were complete (no missing or ambiguous answers). The remaining 17 questionnaires were either missing results for one or more questions, or had some ambiguous answers (*e.g.*, two responses checked for a single question). These errors were an artifact of the conversion from an on-line form to a paper form, where it is easier to miss questions or

have ambiguous and difficult to read answers. In order to include these responses, we determined the personality domain for the missing or ambiguous questions and then removed the results for this user for those domains from further consideration. This left us with $N = 34$ for extraversion, $N = 35$ for neuroticism and openness, $N = 37$ for conscientiousness and $N = 39$ for agreeableness.

The results were analysed using the data collected and scripts written by Dr. Johnson (see `http://www.personal.psu.edu/faculty/j/5/j5j/IPIP/ipipneo120.htm`). His programs calculate scores for each of the 30 facets and five personality domains. It then compares these scores against scores that have been collected over time from a large number of people to determine the percentile into which the respondent falls. The only number reported to the respondent is their percentile score. This would indicate, for example, that a respondent is more extraverted than some percentage of the general population.

We obtained the scripts used on this web site, along with a spreadsheet of the percentile scores on which the calculations are based. The original scripts calculate percentiles where a respondent is compared against others of the same sex and age range. However, we did not collect any demographic information on age, and so modified the scripts to not use this particular data. (We note, however, that this is unlikely to affect our results, given that age was divided into only two groups: 21 and older or younger than 21.) We therefore calculated percentiles using sex as the only discriminator, where these values were based on responses from 7743 men and 13,524 women, representing the results collected by the web site over some period of time. We assume that this population is reasonably close to the general population, although it still suffers from the self-selection bias, which means that we only have results from those people who have access to the study and are willing to take that study, rather than from a truly random population.

We manually entered the data for each respondent via a web page, and recorded the percentile results that were obtained. We grouped the resulting scores into low, medium and high categories, where low indicates that the respondent was below the 30th percentile, high indicates the respondent was above the 70th percentile, with the remainder being the medium. The results from dividing the scores in this manner for both the overall domains and each of their facets are presented in Table I. We also present the results across the five domains for men and women in Tables II and III respectively. We note, however, that the number of women participants in the study is too small to draw any gender-based conclusions.[2] Despite this, women and men were analysed separately as women tend to score higher than men on the domains

of agreeableness and neuroticism, and so need to be compared to other women rather than the population as a whole.

Domain and Facets	Low	Medium	High	Total
Extraversion	13	14	7	34
Friendliness	12	11	11	
Gregariousness	12	15	7	
Assertiveness	4	21	9	
Activity Level	4	13	17	
Excitement-Seeking	22	10	2	
Cheerfulness	11	13	10	
Agreeableness	5	21	13	39
Trust	6	20	13	
Morality	4	13	22	
Altruism	6	22	11	
Cooperation	3	15	21	
Modesty	6	20	13	
Sympathy	12	15	12	
Conscientiousness	1	20	16	37
Self-Efficacy	8	20	9	
Orderliness	11	12	14	
Dutifulness	3	19	15	
Achievement-Striving	3	17	17	
Self-Discipline	7	17	13	
Cautiousness	2	17	18	
Neuroticism	14	13	8	35
Anxiety	11	12	12	
Anger	16	11	8	
Depression	14	13	8	
Self-Consciousness	10	16	9	
Immoderation	8	18	9	
Vulnerability	11	17	7	
Openness to Experience	18	11	6	35
Imagination	23	10	2	
Artistic Interests	12	17	6	
Emotionality	14	14	7	
Adventurousness	15	11	9	
Intellect	8	19	8	
Liberalism	8	10	17	

TABLE I.
THE DISTRIBUTION OF RESULTS AMONG LOW, MEDIUM AND HIGH SCORES FOR THE FIVE DOMAINS AND EACH OF THEIR FACETS.

Personality Domain	Low	Medium	High	Total
Extraversion	8	11	6	25
Agreeableness	3	16	11	30
Conscientiousness	1	14	12	27
Neuroticism	12	8	7	27
Openness to Experience	13	9	4	26

TABLE II.
THE DISTRIBUTION OF RESULTS AMONG LOW, MEDIUM AND HIGH SCORES FOR MEN.

Personality Domain	Low	Medium	High	Total
Extraversion	5	3	1	9
Agreeableness	2	5	2	9
Conscientiousness	0	6	4	10
Neuroticism	2	5	1	8
Openness to Experience	5	2	2	9

TABLE III.
THE DISTRIBUTION OF RESULTS AMONG LOW, MEDIUM AND HIGH SCORES FOR WOMEN.

---

[2]Even when the binning strategy for the percentiles for each domain was changed to only two — low ($< 50\%$) and high ($\geq 50\%$) — the number of female participants is still too low to provide reliable statistical results.

We performed a χ^2 test for significance with two degrees of freedom, comparing our actual results for each domain with the expected results given a uniform random distribution. We assume that the expected result fits a uniform random distribution because we are using percentiles, which is a strict ranking. Therefore we would expect 30% of respondents to have a percentile score on any particular domain of less than or equal to 30 and 30% of respondents to have a percentile score of greater than 70, with the remaining 40% falling between 31 and 70 inclusive.

We examined each domain independently to determine if our respondents differ from the expected values. We found significant differences across two of the five domains. Respondents to our study had unusually high values for conscientiousness ($p = 0.00159$) and unusually low values for openness ($p = 0.0177$). Respondents also generally had high values for agreeableness, with $p = 0.0623$, which suggests that we should examine a larger sample to determine if this might actually be significant or if it is an artifact of our sample size.

Regardless of the significance (or not) of each domain, every domain except neuroticism had at least one facet that showed a significant deviance from a uniform distribution. We start with the two domains that demonstrated significance: conscientiousness and openness. In the domain of conscientiousness, respondents demonstrated significance across three different facets. Unusually high percentiles were found for dutifulness ($p = 0.0162$), achievement-striving ($p = 0.00972$) and cautiousness ($p = 0.00252$). Thus, as a group, our respondents demonstrate that they have a strong sense of duty and obligation, that they work hard and strive towards excellence, and that they take time before making decisions.

In terms of openness, our respondents demonstrate significance on the facet of imagination. Our results show that the survey respondents have a *very* low score for imagination, with $p = 0.00000973$. This implies that our respondents are very much more oriented towards facts rather than fantasy. Additionally, our responses show a strong tendency towards liberalism, although it is not significant ($p = 0.0514$), where this implies that our respondents tend to challenge authority and traditional values. The low p-value here suggests that a larger sample size might indicate if this is truly a significant trait.

Respondents also exhibited significance on two facets in the agreeableness domain. The percentile scores for morality were unusually high ($p = 0.000645$), indicating that the respondents tended to be very sincere and straightforward, demonstrating little need for pretense. Respondents also scored highly for cooperation ($p = 0.000948$), indicating a high willingness to compromise and a desire to avoid confrontations.

While the percentile distribution for extraversion exhibited no significance ($p = 0.412$), there were three facets within extraversion where there was significance. These facets were assertiveness ($p = 0.0237$), activity level ($p = 0.0153$) and excitement seeking ($p = 0.000023$). Respondents showed an unusually high activity level, indicating a busy, fast-paced lifestyle and involvement in a large number of activities. On the opposite extreme, respondents also demonstrated unusually low scores for excitement-seeking, indicating that they do not like commotion and do not tend to be thrill-seeking. The third facet, assertiveness, indicates a person's comfort with speaking out and taking charge. What is interesting about this facet is that respondents scored consistently in the middle range, whereas all other facets that were significant exhibited extremes (*e.g.*, unusually high or unusually low scores). Assertiveness is the only facet where respondents were average.

C. Limitations of the Study

There are a number of limitations of this experiment which must be considered when interpreting our results. First, there is self-selection bias to consider: the questionnaire was handed out to conference attendees, who could choose whether or not to complete and return it. We gathered no data on participants who did not complete the test, which means that we may, for example, have gathered no data on people who had no time to participate, or who dislike completing tests. We are unable to characterize this bias, as we have no data on why individuals did not complete the questionnaire. Thus our results might favour some trait that occurs only in those people who are willing to complete questionnaires, and so not accurately represent the population of conference attendees. This same bias is present in the sample against which the security professionals are compared, as the results from that sample were gathered from participants who took the IPIP NEO test on-line. Thus they both had access to the test and were willing to take it, and so do not represent a truly random sample of the population.

Second, our sample consists only of attendees at the ACSAC conference. Although this group represents a cross-section of the security community, it cannot represent the entire population. Therefore, we cannot generalize to the entire set of security professionals. This is especially true given that we do not know how representative the participants of ACSAC are of the general population of security professionals. Additionally, our sample population is not large: we gathered only 43 responses, three of which had to be discarded.

Although this sample size is small, it is similar to sample sizes used in a number of other five-factor model research studies. These studies have been conducted within various domains, such as mental health (e.g., cognitive impairment (n=48) [3], schizophrenia (n=24) [16], and brain injury (n=21) [22]) and vocational psychology (e.g., burnout (n=36) [30], impression management in job applications (n=22) [1] and working with the disabled (n=48) [23]). Furthermore, other personality research studies within computer science have used similar sample sizes; examples include studies on graphical interface design (n=24) [21], user modelling (n=48) [38], computer-based

documentation preferences (n=32) [35], and information technology teamwork (n=55) [29]. While our sample size is appropriate for our study, and we were able to find statistically significant results, some caution is recommended to avoid over-generalizing our findings.

Finally, despite its popularity, the Five Factor Model is not without controversy. One of the most prominent critics is Block, who faults the model for its lack of grounding in a theoretical model, for its misapplication of factor analysis, and its reliance on self-reporting and restricted laymen's terms in the questionnaires [4], [5]. Proponents of the model have replied to these criticisms, noting that Block ignores much of the evidence that supports the Five Factor Model [8], [13]. Despite dissenting research, support for the Five Factor Model is strong within the psychological community: in general, the evidence in support of the legitimacy of this model of personality is extensive [33]. However, it is worth noting that the debate is by no means resolved, and new theories of personality and personality tests continue to be developed.

IV. DISCUSSION

Survey participants scored high for the conscientiousness domain, and low for the openness domain. The conscientiousness domain relates to spontaneity and acting impulsively, and a high score indicates that respondents are not prone to being impulsive, but are prudent instead. Conscientious individuals are considered to be careful planners, reliable and persistent. However, they can also be perfectionists and workaholics. In particular, survey respondents indicated a strong desire to be recognized as successful, which can also be an indication of being obsessed with work. Additionally, respondents had a strong sense of duty and moral obligation, and tend to think carefully before committing to a decision. It can be argued that these are all good characteristics to have in a security professional, and that a lack of balance in this particular category is not necessarily detrimental to the field. However, this cautiousness may be an issue given events that require a rapid response, such as when an intrusion has been detected. This is especially true given the finding by Cohen [6] that a rapid response time is often a better strategy than having a large number of defences.

On the opposite extreme, survey participants had particularly low scores on the domain openness to experience. This implies that respondents are very practical and down-to-earth, rather than imaginative and creative. At first glance, this domain deals more with the appreciation of art and beauty, and so it may not be surprising that computer security professionals score low on this domain. However, citing from Dr. Johnson's descriptions of the domain [20], a high score on this domain indicates a "facility for thinking in symbols and abstractions" which can take the form of "mathematical, logical, or geometric thinking" in addition to more artistic cognitive styles. Further, it is stated that people with low scores here "may regard the arts and sciences with suspicion, regarding

these endeavors as abstruse or of no practical use." Given that the "intellectual style of the open person may serve a professor well" it is surprising that the survey respondents scored so low on this particular domain. Further, the one facet that was particularly low in this domain was imagination. This particular style of thought and lack of imagination might indicate a weakness in security professionals, and the field might benefit from including more individuals with an open cognitive style as they might be more likely to discover truly new methods to counter cyber-adversaries. However, it is interesting to note that "research has shown that closed thinking is related to superior job performance in police work." Given that computer security and police work could be considered to be related, this may provide some explanation of the low scores on this particular domain.

Other facets on which respondents scored highly included morality and cooperation (both part of the agreeableness domain). It could be argued that high morality is a desired trait in a security professional, as it could be expected that they should not exhibit any deception, nor should they be guarded about providing the whole truth. However, respondents also scored high for cooperation, indicating a dislike of confrontations and a desire to get along well with others. This trait might be desirable in the work-place, but is interesting to find in security professionals given that the profession is founded on confrontation between security professionals and adversaries. However, this can also be viewed that security professionals provide safe-guards to *prevent* confrontations with adversaries. Additionally, scoring high on this facet might indicate that there is a great deal of internal co-operation between security professionals, which in turn is good for the profession as a whole as it is likely that professionals then share solutions to security problems.

Additionally, respondents scored low on the facet for excitement-seeking, indicating that respondents are likely risk-adverse. Greenwald *et al.* [14], in a panel on psychology in security, noted that "a sensation-seeker is a risk taker" and so is more likely to not install or use an InfoSec software package. Thus it is likely a desirable trait that security professionals score low on the excitement-seeking facet.

V. COMPARISON TO RELATED WORK

While a number of articles have been published that relate the five factor model to work performance (*e.g.*, see [2] and [34]), very little seems to have been published relating the five factor model to particular career choices. The literature that does deal with this area has been described as "less well articulated", stating that it is "difficult to formulate hypotheses regarding FFM traits and the nature of employment." [10]

One article that does address this area, however, is by De Fruyt and Mervielde [10]. This article uses the five factor model as a predictor of both employment status and the nature of employment, in combination with the RIASEC model. The RIASEC model is a theory of

vocational personalities that has been developed by John Holland [17]. This model contains six personality types — Realistic, Investigative, Artistic, Social, Enterprising and Conventional — and it is argued that these six types also represent vocational environments. Realistic personalities are considered to be doers, and prefer to work with things rather than people. Investigative personalities are thinkers, who enjoy abstract problems, while artistic personalities are creators who prefer environments where they can exhibit self-expression. Social personalities are concerned with the welfare of others, and are responsible and helpful. Enterprising personalities are persuaders who enjoy leading, speaking and selling, while conventional personalities are organizers who are conservative and orderly. (These descriptions have been adapted from `http://edtech.jmu.edu/bis/RIASEC.htm`.) De Fruyt and Mervielde [10] found that a low score on openness predicts employment in a realistic vocation. Sample vocations in this domain include electrical engineers, software technicians and police officers. They also found that a high score on conscientiousness also predicted work in realistic vocations. Interestingly, computer analyst, which should require similar traits to a security professional, is an investigative vocation and not a realistic one.

While little has been published comparing the five factor model to career choices, there are numerous articles comparing the Myers-Briggs Type Indicator (MBTI) to career choices. In a previous paper, we analysed the MBTI types of 79 security professionals [11]. The MBTI consists of four dichotomous domains —- extraversion/introversion (EI), thinking/feeling (TF), sensing/intuiting (SN) and judging/perceiving (JP) — resulting in 16 personality "types". We found that security professionals are different from the general population of the United States across all four dichotomies, tending to be more introverted, intuiting, thinking and judging. In particular, we found a predominance of INTJ types, who tend to be "perfectionists who value personal competence and their own original ideas." We also noted a very strong preference in our sample for intuition (85.5%), which is markedly different from the general population (32%). This indicates a strong preference for focusing on meanings and possibilities, and a low preference for dealing with details or observable phenomenon.

Several comparisons have been made between the five factor model (FFM) and the Myers-Briggs Type Indicator (MBTI), which has been summarized by Gruber [15]. He notes in this article that FFM extraversion is related to the MBTI extraversion/introversion dichotomy, and Openness is related to the sensing/intuiting dichotomy, with a high score here indicating intuition. The thinking/feeling dichotomy is related to agreeableness, with a high score in agreeableness being related to feeling and a low score to thinking. Finally, the judging/perceiving dichotomy is similar to conscientiousness, with a high score being similar to judging and a low score to perceiving.

Using the mappings outlined in [15], a low score on openness indicates MBTI sensing types, a high score on conscientiousness indicates MBTI judging types, and a high score on agreeableness indicates MBTI feeling types. This results in type xSFJ. Examining the relationships identified by McCrae and Costa [26], the thinking/feeling dichotomy is less clear: while a high score on agreeableness is positively correlated with feeling types, a high score on conscientiousness is *negatively* correlated with feeling types. However, MacDonald *et al.* [25] find the correlation between agreeableness and feeling (0.52) to be significant, while the negative correlation between conscientiousness and feeling is not (-0.02). MacDonald *et al.* [25] also found that intuiting was positively correlated with agreeableness, however we did not use this result to strongly influence our hypothesized corresponding MBTI type as it was not found by McCrae and Costa [26].

We found that our result (MBTI type xSFJ) is different across two dichotomies from the result found in our earlier work on a similar sample population [11]. Our respondents demonstrated a very low score for openness indicating a very sensing-based population. This is markedly different from the previous study, which found that the security population was extremely high in intuiting. Similarly, we found that our population is more predisposed to be the feeling type, while the previous population was high on the thinking scale.

These differences are unusual, and require some explanation. One possible explanation is that the mappings between the MBTI and FFM models are not particularly accurate. For example, the MBTI indicates that someone who is feeling tends to make decisions based on social considerations while someone who is thinking focuses on facts. This does not map well to agreeableness, which deals more with how people relate to others and not with what factors they consider when making decisions. For example, someone who tends towards facts and figures is not necessarily uncooperative or immodest.

Another possible explanation could be related to size of the sample population and the limited number of questions used in the FFM survey. For example, many of the questions regarding openness to experience could be interpreted more harshly given the audience. One example here is the trait "enjoy theoretical conversations." This might have been interpreted with the more narrow view of computer science theory, and less with the more broad view of "what if" types of conversations. Similarly, one of the questions was "enjoy going to art museums", which is again very specific. It might be the case that, while respondents do not enjoy going to art museums, they might enjoy going to the symphony, and so answering no to this question does not necessarily reflect an overall lack of artistic interest. Thus it might be the case that the 240-question version of the survey would provide different results than the 120-question version.

Another possibility is that, while the sample population for both this study and our previous study [11] consisted of security professionals, the sampling strategy resulted in very different people responding. For example, we sampled here from the Annual Computer Security Appli-

cations Conference, which could imply that we are more likely to encounter individuals concerned with the applied aspects of security and so have lower scores on openness and are therefore more sensing in MBTI parlance. In contrast, the previous study sampled from among primarily academic contacts, and so the respondents might be more likely to be intuiting.

VI. FUTURE WORK

One of the limitations of this study stems from the size of the sample and the non-random nature of the pool from which participants were chosen. As a result, caution must be used in extending these results to the security profession as a whole. However, the results from this study indicate that there may be particular personality traits that are dominant within the security community, and thus future studies are worth pursuing. Such future studies would need to address the limitations of this study, and so would need to consist of a larger sample size that is chosen randomly from the sample of all security professionals. While obtaining a list of all security professionals may not be possible, it might be possible to leverage professional associations, such as ACM, IEEE, SANS and (ISC)^2, in order to cover a broad spectrum of professionals.

In repeating the study with a larger sample, other improvements to the current study should also be incorporated. For example, the test should be performed on-line, in order to prevent ambiguous or missing responses. The use of the original NEO PI-R [31] should also be considered, as it contains more questions and will thus produce more accurate results.

Finally, much of our discussion of the results has focused on how any dominant personality traits might affect the profession as a whole, in particular in the context of developing effective security solutions. However, this discussion is largely based on speculation. Therefore a follow-up study should be conducted that investigates the impact that particular personality traits have on job performance.

VII. CONCLUDING REMARKS

Our Five Factor Method analysis of security professionals revealed some interesting dominant personality traits. In particular, participants scored high in the conscientiousness domain, and low in the openness domain. Having highly-conscientious defenders appears to be beneficial, as it indicates caution, a tendency to plan, and thoroughness. However, it may also be the case that security professionals may not respond quickly in time critical situations such as when an intrusion has occurred. The low score in the openness to experience domain could indicate rigidness of thought, although the questionnaire focuses mainly on artistic sensibilities rather than general acceptance of unusual ideas. However, this aspect is generally high in professors and researchers, which may indicate that security professionals may not be inventive in creating new security mechanisms.

Security professionals also demonstrated significant deviances in some of the individual facets within every domain except neuroticism. For example, respondents had a *very* low score for imagination, which is related to the low score on openness to new ideas. Respondents scored very highly on co-operation, which is unusual given that the field is inherently one of conflict, of defenders versus adversaries. The high level of co-operation might be a good trait, indicating that security professionals tend to work well together. Alternatively, it might reflect a weakness given the aversion to conflict. Security professionals also scored unusually high on the facet for activity level, indicating the preference for a busy life-style with the need to balance many activities. If security professionals have positions that mimic their personality preferences, then this could possibly result in the professional being subject to missing important security information due simply to not having the time or inclination to focus on any one particular area.

One additional finding is that the majority of our respondents were not excitement seeking (p = 0.00002304); this indicates a risk-averse population. Again, this may be desirable in a security group: one is attempting to reduce the risk and consequences of a security breach. However, it may also signify that defenders take conservative approaches when they tackle a problem, fearing a negative outcome. It may be necessary to create organizational structures where "contained failure" is supported, so that experimental approaches can be developed without the possibility of actual system damage.

Future studies should be performed to determine if the results discovered in the study from the participants at the 2004 Annual Computer Security Applications Conference are more generally representative of the security profession. Additionally, assuming that such dominant personality traits are still present, follow-up studies need to be performed to determine the exact impact this has on job performance and if our hypotheses on the weaknesses such traits might create in the security field are indeed correct.

VIII. ACKNOWLEDGMENTS

REFERENCES

[1] R. Bagby and M. Marshall. Positive impression management and its influence on the Revised NEO Personality Inventory: a comparison of analog and differential prevalence group designs. *Psychological Assessment*, 15(3):333–339, 2003.

[2] M. Barrick and M. Mount. The big five personality dimensions and job performance: A meta-analysis. *Personnel Psychology*, 44:1–26, 1991.

[3] R. H. Benedict, R. L. Priore, C. Miller, F. Munschauer, and L. Jacobs. Personality disorder in multiple sclerosis correlates with cognitive impairment. *Journal of Neuropsychiatry and Clinical Neurosciences*, 13(1):70–76, 2001.

[4] J. Block. A contrarian view of the five-factor approach to personality description. *Psychological Bulletin*, 117(2):187–215, 1995.

[5] J. Block. Going beyond the five factors given: Rejoinder to Costa and McCrae (1995) and Goldberg and Saucier (1995). *Psychological Bulletin*, 117(2):226–229, 1995.

[6] F. Cohen. Simulating cyber attacks, defenses, and consequences. http://www.all.net/journal/ntb/simulate/simulate.html, 1999. Last visited: 5 April 2002.

[7] P. T. Costa Jr. and R. R. McCrae. NEO PI-R: Professional Manual. Technical report, Psychological Assessment Resources, Odessa, FL, 1992.

[8] P. T. Costa Jr. and R. R. McCrae. Solid ground in the wetlands of personality: a reply to Block. *Psychological Bulletin*, 117(2):187–215, 1995.

[9] D. Fiske. Consistency of the factorial structures of personality ratings from different sources. *Journal of Abnormal Social Psychology*, (44):329–344, 1949.

[10] F. D. Fruyt and I. Mervielde. RIASEC types and big five traits as predictors of employment status and nature of employment. *Personnel Psychology*, 52(3):701–727, 1999.

[11] C. Gates and T. Whalen. Profiling the defenders. In *Proceedings of the 2004 New Security Paradigms Workshop*, pages 107–114, Nova Scotia, Canada, 2004. 20-23 September 2004.

[12] L. Goldberg. A broad-bandwidth, public domain, personality inventory measuring the lower-level facets of several five-factor models. In *Personality Psychology in Europe*, volume 7, pages 7–28, Tilburg, The Netherlands, 1999. Tilburg University Press.

[13] L. Goldberg and G. Saucier. So what do you propose we use instead? A reply to Block. *Psychological Bulletin*, 117(2):187–215, 1995.

[14] S. J. Greenwald, K. G. Olthoff, V. Raskin, and W. Ruch. The user non-acceptance paradigm: Infosec's dirty little secret. In *Proceedings of the 2004 New Security Paradigms Workshop*, pages 35–43, Nova Scotia, Canada, 2004. 20-23 September 2004.

[15] G. P. Gruber. Standardized testing and employment equity career counselling: A literature review of six tests. http://www.psc-cfp.gc.ca/ee/eecco/pdf/standardized_e.pdf, 2000. Prepared for The Employment Equity Career Development Office, Public Service Commission of Canada. Last visited: 2 June 2005.

[16] R. Gurrera, P. Nestor, and B. O'Donnell. Personality traits in schizophrenia: Comparison with a community sample. *Journal of Nervous and Mental Disease*, 188(1):31–35, 2000.

[17] J. Holland. *Making Vocational Choices: A Theory of Vocational Personalities and Work Environments*. Prentice-Hall, Englewood Cliffs, NJ, 1985.

[18] International Personality Item Pool. A scientific collaboratory for the development of advanced measures of personality traits and other individual differences. http://ipip.ori.org/, 2001. Last visited: 1 June 2005.

[19] J. A. Johnson. Descriptions used in IPIP-NEO narrative report. http://www.personal.psu.edu/faculty/j/5/j5j/IPIPNEOdescriptions.html, 2004. Last visited: 2 June 2005.

[20] J. A. Johnson. IPIP-NEO narrative report. http://www.personal.psu.edu/faculty/j/5/j5j/IPIP/shortipipneo3.cgi, 2005. Last visited: 1 June 2005.

[21] A. Karsvall. Personality preferences in graphical interface design. In *Proceedings of the Second Nordic Conference on Human-Computer Interaction*, pages 217–218, Aarhus, Denmark, 2002. 19-23 October 2002.

[22] J. Kurtz, S. Putnam, and C. Stone. Stability of normal personality traits after traumatic brain injury. *Journal of Head Trauma Rehabilitation*, 13(3):1–14, 1998.

[23] E. R. Lawrence, L. M. Glidden, and B. M. Jobe. Keeping them happy: Job satisfaction, personality, and attitudes toward disability in predicting counselor job retention. *Education and Training in Developmental Disabilities*, 41(1):70–80, 2006.

[24] R. Likert. A technique for the measurement of attitudes. *Archives of Pyschology*, (140):55, 1932.

[25] D. A. MacDonald, P. E. Anderson, C. I. Tsagarakis, and C. J. Holland. Examination of the relationship between the Myers-Briggs Type Indicator and the NEO personality inventory. *Psychological Reports*, 74:339–344, 1994.

[26] R. R. McCrae and P. T. Costa Jr. Reinterpretting the Myers-Briggs Type Indicator from the perspective of the five-factor model of personality. *Journal of Personality*, 57(1):17–40, 1989.

[27] National Science Foundation. Women, minorities, and persons with disabilities in science and engineering - 2002: Employment. http://www.nsf.gov/sbe/srs/nsf03312/c6/c6s3.htm. Last visited: 10 April 2004.

[28] W. Norman. Toward an adequate taxonomy of personality attributes: Replicated factor structure in peer nomination personality ratings. *Journal of Abnormal and Social Psychology*, (66):574–583, 1963.

[29] A. R. Peslak. The impact of personality on information technology team projects. In *Proceedings of the 2006 ACM SIGMIS CPR Conference on Computer Personnel Research*, pages 273–279, Ponoma, USA, 2006. 13-15 April 2006.

[30] R. L. Piedmont. A longitudinal analysis of burnout in the health care setting: The role of personal dispositions. *Journal of Personality Assessment*, 61(3):457–473, 1993.

[31] Psychological Assessment Resources, Inc. NEO Personality Inventory-Revised (NEO PI-R). http://www3.parinc.com/products/product.aspx?Productid=NEO-PI-R. Last visited: 1 June 2005.

[32] M. Rogers. *A Social Learning Theory and Moral Disengagment Analysis of Criminal Computer Behavior: An Exploratory Study*. PhD thesis, University of Manitoba, 2001.

[33] J. Rolland, W. Parker, and H. Stumpf. A psychometric examination of the French translations of the NEO-PI-R and NEO-FFI. *Journal of Personality Assessment*, 71(2):269–291, 1998.

[34] J. Salgado. The five-factor model of personality and job performance in the European community. *Journal of Applied Psychology*, 82:30–43, 1997.

[35] K. Sayles and D. G. Novick. Assessing effectiveness of personality style in documentation. In *Proceedings of the 22nd Annual International Conference on Design of Communication*, pages 75–82, Memphis, USA, 2004. 10-13 October 2004.

[36] E. Shaw, K. Ruby, and J. Post. The insider threat to information systems: The psychology of the dangerous insider. *Security Awareness Bulletin*, 2-98:1–10, 1998.

[37] E. Tupes and R. Christal. Recurrent personality factors based on trait ratings. Technical Report ASD-TR-61-97, Lackland Air Force Base, TX: Aeronautical Systems Division, Personnel Laboratory, 1961.

[38] X. Zhou and C. Conati. Inferring user goals from personality and behavior in a causal model of user affect. In *Proceedings of the Eighth International Conference on Intelligent User Interfaces*, pages 211–218, Miami, USA, 2003. 12-15 January 2003.

Tara Whalen is a doctoral candidate at Dalhousie University in Nova Scotia. She previously worked in network security at the Communications Research Centre Canada. Her current research interests include human factors in security, computer-supported cooperative work, privacy, and the social implications of technology.

Carrie Gates is a researcher with CA Labs in New York, having received her PhD in the area of computer and communications security in May 2006 from Dalhousie University. Previously, she worked as a security researcher at CERT, Carnegie Mellon University. Her current research interests include security, privacy and usability.