INL/CON-15-37384
PREPRINT

Investigating the Relationship between Need for Cognition and Skill in Ethical Hackers

7th International Conference on Applied Human Factors and Ergonomics (2016)

Katya Le Blanc and Sarah Freeman

July 2016

The INL is a
U.S. Department of Energy
National Laboratory
operated by
Battelle Energy Alliance

Investigating the Relationship between Need for Cognition and Skill in Ethical Hackers

Katya Le Blanc[1] and Sarah Freeman[1]

[1] Idaho National Laboratory, 2525 Fremont Avenue, Idaho Falls, ID, 83402, USA
{Katya.LeBlanc, Sarah.Freeman}
@inl.gov

Abstract. As technology gets more complex and increasingly connected, there is a continuing concern with cyber security. Partnered with this concern is continuing demand for cyber security defenders. Unfortunately, there is currently a dearth of skilled professionals to meet that demand. In order to prepare the next generation of cyber defenders, we need to understand what characteristics make skilled cyber security professionals. For this work, we focus on professionals who take an offensive approach to cyber security, so called ethical hackers. These hackers utilize many of the same skills that the adversaries that we defend against would use, but with the goal of identifying vulnerabilities so they can be mitigated before they are exploited by adversaries. We interviewed cyber security researchers who specialize in offensive approaches. Based on the responses to the hacker skill inventory, we generated a self-reported skill score for each participant. We also developed a peer-rating for each participant based on the number of times each individual that was interviewed was named as the most skilled in a particular area. The results are discussed in the context of training and recruitment of cyber security professionals.

Keywords: Cyber security · Hackers · Attribution · Human Factors

1 Introduction

Recent years have seen explosion of threat-focused research aiming to meet the challenges of an evolving cyber landscape. Organizations, both public and private, have sought to advance threat analysis processes, methodologies, and capabilities in order to improve defender capabilities. Unfortunately, these capabilities have failed to match the speed of evolution of the cyber adversary, as defense is always harder than offensive action. Compounding this problem is a consistent dearth of suitable cyber talent due to an inherent misunderstanding of these individuals.

Understanding what characteristics make skilled cyber researchers can help prepare the next generation of cyber security professionals, as well as help to train and identify the next generation of cyber defenders. For this work, we focus on professionals who help secure systems by taking an offensive approach to cyber security, otherwise known as ethical hackers. These hackers utilize many of the same skills that the ad-

versaries we defend against would use, but with the goal of identifying vulnerabilities so they can be mitigated before they are exploited by those adversaries.

Previous work in this area has typically focused on the identification of individual adversary profiles, for example the "insider" or "cyber terrorist." Unfortunately, the majority of this work also reveals a pervasive bias that limited understanding of the group. For example, as noted by Thomas Holt, the motivations of individual hackers are often oversimplified and reduced to efforts of economic gain or expansion of social status.[1] This distortion is likely the result of the focus areas of this research, for example, social science research that aims to understand the motivation behind cyber attacks or the development of malware. However, by focusing on malicious or illegal cyber activity, this research narrows the scope of motivations and ignores a large component of the cyber security community.

One notable effort was MITRE's 2013 piece, "Mapping the Cyber Terrain." The MITRE research team conducted a survey of previous research and summarized adversary characteristics, dividing them into three main areas: capability, intent, and target. Additionally, some modest efforts have been undertaken to describe the human components of an attack, namely the willingness of an individual to engage in risky behavior based on existing skill sets. While this research highlights the potential benefit of work in this field, it also fails to recognize the nuances in the adversarial approach. The skill sets of the hacker (both blackhat and whitehat) are not developed within a vacuum, but through the commingling and cross-pollination of peers and competitors. Understanding the natural learning process for these individuals is required for the development of the next generation of cyber defenders.

One critical aspect of cyber learning and cyber education is distinguishing between what can be taught and the inherent manifestation of a particular personality. For example, what is the significance of an individual's drive or natural curiosity and how does it impact a hacking skill in a variety of facets. By understanding these distinctions, education can be altered to ensure not only the most effective training mechanism is used but that those individuals with appropriate aptitude are identified.

The purpose of this work is to identify the critical characteristics of a skilled hacker. A commonly held belief among ethical hackers is that hackers must possess exceptional curiosity and problem solving skills in order to be successful. Curiosity has been studied extensively in psychology, but there is no consensus on what it is and how to measure it. Further, many existing inventories for assessing curiosity are targeted at measuring curiosity in children. Although there is no accepted standard to assess curiosity in adults, a related construct, called Need for Cognition, may capture what is meant when people speak of curiosity. The Need for Cognition scale also captures the tendency toward preferring complex problems (which correlates with good problem solving skills), and may provide insight into what makes skilled hackers. We used the Need for Cognition scale to assess Ethical Hacker's curiosity.

In addition to the Need for Cognition, we used a structured interview to assess hacker skill. Hackers rated their own skill on a scale from one to ten on a predefined list of hacker skills. The participants were then asked to rate peers who they felt were most skilled in each of the areas. They rated two peers for each skill, one that they worked with directly and one that was the most skilled in the field (these could be known by reputation only). The hypothesis was that hackers have a higher than aver-

age (i.e., compared to non-hackers) Need for Cognition and that Need for Cognition will be positively correlated with self-reported and peer-reported skill.

2 Method

2.1 Participants

Participants included 14 individuals who were identified as cyber security researchers. Thirteen of the participants were male and one was female. The mean age was 35 years. Out of the total amount of participants, 14% had attended no college, 57% had a bachelor's degree and 29% had a masters or higher. Participants had an average of 11 years technical experience conducting tasks related to hacking.

2.2 Procedure

The testing procedure consisted of two components, a structured interview protocol and the Need for Cognition Scale. Researchers worked with subject matter experts to develop the interview questions. The structured interview investigated several aspects including hacker experience, skills, use of technology, ethics, paranoia, and other preferences related to technology use. A portion of the structured interview was devoted to assessing self-reported and peer reported skill. To assess self-reported skill, each participant was asked to rate his or her skill on a set of predetermined categories on a scale of 1 to 10. The skills included:

- Reverse Engineering
- Cryptography
- Penetration Testing
- Code Review
- Scripting
- Exploit Writing
- Social Engineering

To assess peer-reported skill for each of the categories, participants were asked to name their peer who is the most skilled in each of the categories and provide a rating from 1 to 10. The researchers chose this method of peer rating because they were advised that the participants would not be comfortable rating each of their peers individually, but they may feel comfortable naming the person that they find most skilled. Further, this method allowed researchers to obtain a peer score without restricting the participant pool. The obvious limitation of this method is that it does not yield a score for each of the participants, but only provided scores for the people who were deemed most skilled by one or more of the participants.

In addition to the structured interview questions, the researchers selected the*Need for Cognition Scale (NFC)*, developed by Cacioppo and Petty in 1982, to evaluate individuals on their tendency to engage in (and enjoy) a variety of cognitive activities. Research suggests that individuals who score high on this scale "tend to think carefully and extensively about information they encounter and enjoy effortful cognitive

endeavors."[2] In contrast, those individuals who score lower on this scale "tend to avoid such endeavors, thinking only superficially about information they encounter."[2]

3 Results

3.1 Need for Cognition Scores

The Need for Cognition scores (NFC) were calculated for each participant as an average of each of the individual items on the scale (reversing the score for appropriate items). The mean need for cognition score was $M = 4.02$, $SD = .47$ on a five point scale.

3.2 Self-Reported Skill

Self- reported skill was assessed for each of the skills listed in the interview form. The means across participants for each of the skills are reported in table 1.

Table 1. Self-reported scores range from 1 (least skilled) to 10 (most skilled).

Skill	Mean Self-reported Score	Standard deviation
Reverse Engineering	6.5	1.9
Cryptography	3.5	1.9
Penetration Testing	5.1	2.5
Code Review	5.3	2.9
Scripting	6.9	1.9
Exploit Writing	5.4	2.3
Social Engineering	3.9	2.8

On average, the participants reported that they were most skilled at reverse engineering and scripting and least skilled at cryptography and social engineering. In order to assess the relationship between NFC and self-reported skill, the researchers computed an aggregate skill score for each participant. The average aggregate self-reported score for skills was $M = 5.5$, $SD = 1.5$.

3.3 Peer-Reported skill

Because of the limited data for the peer ratings, the researchers collapsed the peer-rating score across all of the skill categories. A peer-score was computed for each participant. To compute the peer-score, the researchers counted the total number of times that each participant was named as most skilled by another participant in any of the skill categories. This number serves as the peer score, and varies from zero (for participants who were never named as the most skilled by another participant) to 98

(the maximum number of times that a participant could be named by one of the 14 participants for all seven categories).

Participants were named an average of 3.4 times by their peers. The scores varied from zero to 16. Six participants were not named as the most skilled by any of their peers for any of the skill categories. The other eight participant's scores varied from one to 16.

3.4 Relationships Between Scores and Need for Cognition

According to the belief that high curiosity is a prerequisite for skilled hackers, one would expect a strong relationship between hacker skill scores and results of the NFC scale. The researchers used non-parametric tests to assess the relationship between self-reported scores and peer-reported scores and each score's relationship to Need for Cognition. The researchers used an alpha level of .10 for the tests to compensate for the relatively small sample size.

First, to assess how well individuals own rating aligned with their peer scores, the researchers conducted a Spearman's' Rho test to determine the relationship between peer-reported score and self-reported score. The test revealed that they were not related and the correlation was not significant at a p =.10.

Next the aggregate self-reported ratings and NFC scores were subjected to a Spearman's Rho test and the results revealed that there was no significant relationship between self-reported hacker skills and NFC.

Finally, the researchers conducted a Spearman's Rho test on the relationship between the peer scores and NFC. The test revealed a weak relationship between NFC and Peer scores $\rho = .45$, $p = .106$.

4 Discussion and Conclusions

The purpose of this work was to investigate whether hackers had an intrinsic desire to seek out thinking and solve difficult problems through the Need for Cognition Scale. The results indicate that hackers have a high NFC. The results however, do not indicate a relationship between NFC and self-reported or peer reported skill among the hacker population. The results showed only a weak relationship between NFC and peer-reported skill.

The lack of a detectable relationship between NFC and skill scores could be due to many limitations present in this study. First, the sample size (14 participants) was small and limited statistical power. Second, the method for collecting peer scores yielded no score for about half the participants, which limits the degree to which the scores varied making it difficult to detect a relationship between peer scores and NFC scores. The fact that we did detect a weak relationship between the two indicates that with a study more participants that also utilizes a method that generates a peer-reported skill score for each participant, might yield an understanding of the relationship between peer ratings and NFC.

NFC was not a strong predictor of skill among hackers based on this work; however it may be an effective way to identify individuals who are suited to the types of tasks that cyber defenders will need to secure our critical infrastructure.

Acknowledgements

This research was funded by Idaho National Laboratory (INL) and the Department of Energy through laboratory directed research and development funds. INL is a Federally Funded Research and Development Center (FFRDC) managed by Battelle Energy Alliance (BEA) for the Department of Energy. This manuscript has been authored by Battelle Energy Alliance, LLC under Contract No. DE-AC07-05ID14517 with the U.S. Department of Energy. The United States Government retains and the publisher, by accepting the article for publication, acknowledges that the United States Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this manuscript, or allow others to do so, for United States Government purposes.

References

1. Holt, Thomas: The Attack Dynamics of Political and Religiously Motivated Hackers. In: Proceedings of the Cyber Infrastructure Protection, pp. 159—180. City University of New York, New York (2009)
2. Bizer, George Y., Krosnick, Jon A., Petty, Richard E., Rucker, Derek D., Wheeler, S. Christian: Need for Cognition and Need to Evaluate in the 1998 National Election Survey Pilot Study. Technical paper, The Ohio State University (2000)