http://dx.doi.org/10.7840/kics.2016.41.4.489

해커들의 심리변인에 기반한 탈선적 해킹활동 및 해킹타입 예측 모델

박 찬 현◆, 송 인 욱*, 김 민 지*, 장 은 희*, 허 준**, 김 현 택°

Prediction Model for Deviant Hacking Behavior and Hacking Type in Hackers Based on Psychological Variable

Chan Hyun Park◆, In Uk Song*, Min Ji Kim*, Eun Hee Chang*, Jun Heo**, Hyun Taek Kim°

요 약

정보복제 및 도/감청이 기술적으로 불가능한 양자통신의 출현에도 불구하고, 일부 해커들의 부적절한 동기와 목적에 의한 사이버테러(cyber-terror)는 지속적으로 시도될 것으로 예상된다. 따라서 해킹의 주체인 해커들의 심리적 관점에 대한 연구의 중요성과 필요성이 더욱 커지고 있다. 본 연구는 Beebe & Clark(2006)의 연구를 보완하여, 탈선적 해킹에 관련된 해커들의 주요한 심리적 독립변수가 무엇인지 탐색하고, 그에 따른 해킹의도와 실제 해킹경험을 종속변수로 측정하였다. 본 연구의 결과로서, 해킹의도와 해커들의 타입을 구분해서 예측할 수 있는 모델을 도출하였으며, 이 결과는 향상된 사이버 보안을 위한 인적 관리에 응용할 수 있음을 제안하였다.

Key Words : Hacker, Psychology, Security, Prediction model, Cybercriminology

ABSTRACT

Despite the extant quantum communication technology that does not allow copying, wiretapping, and/or monitoring, cyber-terror-attempts from hackers with unconscientious purposes and motives are prospected to persist. Hence, it is imperative and necessary to invest in studies geared toward understanding the psychology of hackers. The current study referred to Beebe & Clark (2006) and sought out the psychological variables in hackers involved in deviant hacking activities, measured the purpose of hacking and actual hacking experiences, and constructed a predictive model that can categorize hacker types based on their intentions.

Ⅰ. 서 론

양자암호통신은 보안키를 송/수신자가 안전하게 나누어 가질 수 있는 양자키 분배(quantum key distribution) 기술로서, 이론적으로 정보복제 및 도/감청이 불가능하다. 그러나 Xu 외(2010)[1]는 암호송신자가 이전 비트와 다른 편광 방향을 갖는 비트를 보내려 할 때 발생하는 시간차를 이용하여 해커가 비트를 낚아채고 비트들의 편광 방향을 은밀하게 바꿔 보낼 수 있음을 밝혀냈다. 이를 통해 도청으로 인해 발생하

※ 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ITC연구센터육성 지원사업의 연구결과로 수행되었음 (IITP-2016-R0992-16-1017)
◆ First Author : Dep. of Psychology, Korea University, fr33bird@naver.com, 학생회원
° Corresponding Author : Dep. of Psychology, Korea University, neurolab@korea.ac.kr, 정회원
* Dept. of Psychology, Korea University, songiu1@korea.ac.kr, goal1110@naver.com, eh860@hanmail.net
** School of Electrical Engineering, Korea University, junheo@korea.ac.kr, 종신회원
논문번호 : KICS2016-02-033, Received February 190, 2016; Revised April 19, 2016; Accepted April 19, 2016

는 오류를 낮춤으로써 들키지 않고 암호를 해킹할 수 있었다. 이후 많은 양자통신 해킹 시도가 있었는데[2-5], 이는 앞으로도 특정 해커들의 부적절한 동기와 목적에 의한 사이버 범죄가 지속될 것이라는 점을 시사한다.

하지만 지금까지 해킹에 대한 연구는 대부분 기술적인 관점에 치중되어 왔으며, 해커에 대한 심리학적 관점의 접근은 미미한 상황이다. Rogers(2003)[6]는 사이버 범죄에 대한 연구 중, 사이버 범죄자의 성격 특성이나 개인차, 동기, 행동적 요소들에 초점을 맞춘 심리학적 연구가 거의 없다는 점을 지적했으며, Rose(1999)[7]는 해킹을 포함한 사이버 범죄에 대처하기 위해서는 왜 해킹이 일어나는지 알아내서 해킹을 하고자하는 동기를 감소시키는 전략을 발전시켜야 한다고 제안했다. 또한 Buyens 외(2007)[8]는 공격자 프로필(attacker profiles)을 개발하는 것이 비용 면에서 해킹범죄에 대처하는 가장 효율적인 전략이라고 주장했다. 이는 매년 사이버 테러를 포함한 다양한 사이버 범죄를 저지르는 주체인 해커를 심리학적으로 연구하는 것에 대한 중요성과 필요성을 시사한다.

Beebe & Clark(2006)[9]는 어떠한 윤리성향을 가진 해커들이 범법적(illegal) 해킹태도와 해킹의도를 가지는지에 대한 간단한 예측모델을 제시하였다(그림 1). 이 모델은 해커들의 인구통계학적 정보와 Forsyth (1980)[10]가 제안한 윤리적 개념척도로 그들의 해킹태도(범법적 해킹에 용인적인 태도)를 예측하고, 추출된 태도점수를 통해 실제 해킹의도(범법적 해킹을 저지를 의향)를 예측하여 그에 따른 잠재적 해커타입(Blackhat, Ex-blackhat, Whitehat, Nohat)을 분류할 수 있는 모델이다.

하지만 해당 연구에서 사용한 해커들의 심리변수는 윤리성향에 국한되어 있으며, 종속변수로 사용한 해킹

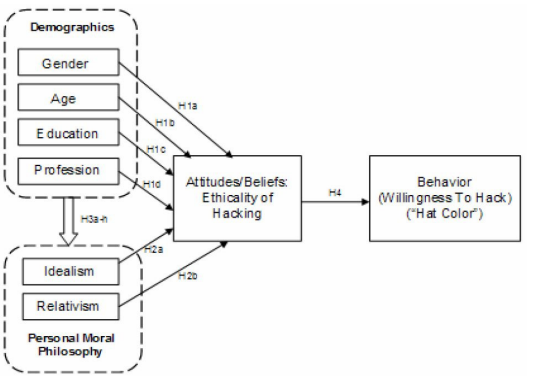


그림 1. Beebe & Clark(2006)의 해킹 예측 모델
Fig. 1. A Model for Predicting Hacker Behavior by Beebe & Clark(2006)

의도 또한 해커들의 실제 해킹활동여부를 측정한 것이 아닌, 탈선적 해킹에 대한 의도만을 측정했다는 점에서 예측모델로서는 그 한계가 있다. 잘 알려진 바대로, 인간의 심리적 특성은 윤리성향 외에 성격, 기질, 동기 등 다양한 특성들을 포괄적으로 포함하고 있기 때문에, 이러한 심리변수들 중에서 어떤 변수가 실제 해커들의 탈선적 해킹태도에 가장 큰 영향을 미치는지 확인하는 과정이 요구된다. 또한 좋은 예측모델은 탈선적 해킹행동에 대한 의도뿐만 아니라 해커들의 실제 해킹경험 또한 예측할 수 있어야 그 설명력이 증가한다.

본 연구진은 Beebe & Clark(2006)가 수립한 해킹 예측모델을 기반으로 하여, 해커심리에 대한 선행 연구들의 이론적 배경과 결과들[11-13]을 참고한 보완된 모델을 수립하였다(그림 2). 보완된 모델은 기존 모델이 측정한 해커들의 윤리성향 외에 탈선적 해킹에 영향을 주는 심리변수들이라고 알려진 최적몰입경험(Flow), 공격적 기질과 반응(Angry Temperament and Angry Reaction), 위험감수성(Risk propensity), Big-5 성격유형, 총 4개의 심리변수들을 모델의 독립변수에 추가적으로 사용하였다. 종속변수에는 기존의 해킹의도 외에 해커들의 실제 해킹경험(해킹빈도, 해킹활동유형)에 대한 변수들을 추가하여 보다 포괄적인 연구모델을 수립하였다.

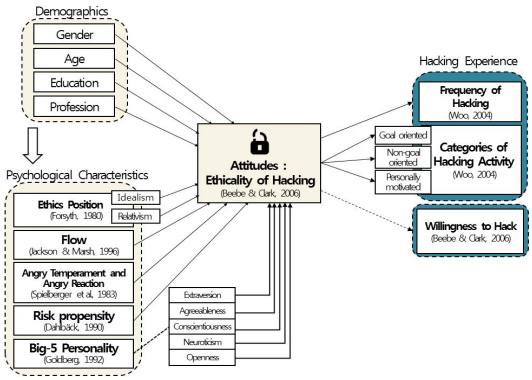


그림 2. 본 연구진이 보완한 연구모델
Fig. 2. A complemented research model

Ⅱ. 실 험

2.1 연구대상

서울소재 대학 내에서 해킹기술을 보유한 정보보안 관련전공 학과생 및 모의해킹 동아리생 71명을 오프라인으로 모집하였다. 또한 국내 모의해킹 커뮤니티

(www.hackerfactory.co.kr)와 정보보안 커뮤니티 (www.securityplus.or.kr)의 협조를 받아 온라인 커뮤니티에서 활동하는 해커 20명을 모집하였다.

2.2 연구방법

피험자들은 본 연구진이 제작한 심리척도지에 답하였다. 자신의 신분노출을 경계하는 해커들의 특성상 오프라인 설문은 모임관계자의 참석 아래 비공개로 진행되었다. 온라인 설문은 구글독스(https://docs.google.com)를 사용해 제작했으며, 각 온라인 커뮤니티 운영진의 협조를 구하여 게시판에 설문을 게재하였다. 데이터 수집은 2015년 11월 1일부터 2016년 1월 10일까지 이루어졌다. 설문은 어떠한 개인정보도 수집하지 않았으며, 위 사실을 설문 전에 충분히 공지하였다. 설문 데이터파일들은 보안을 위해 인터넷이 연결되지 않은 PC에 보관하였다. 본 연구의 실증분석은 모두 유의수준 p<.05에서 검증하였으며, 통계분석에는 SPSS-WIN 22.0 프로그램을 사용하여 분석하였다.

2.3 측정변수

독립변수는 인구통계학적 정보(성별, 연령, 학력수준, 전문성)와 함께 윤리성향, 최적몰입경험, 공격적 기질과 반응, 위험감수성향, Big-5 성격유형을 측정하였다. 종속변수로는 해킹경험(해킹빈도, 해킹활동유형)과 해킹의도를 측정하였으며, 종속변수를 매개하는 변수로는 해킹에 대한 태도를 측정하였다(표 1).

각 변수들의 판별 타당도를 검증하기 위해 직각회전 주요인분석(varimax principal components factor analysis)을 사용하였으며, 아이겐 값 1.0이상, 요인적재량(Factor loading) ±.50이상을 기준으로 하여 기준 이하의 문항들을 제거하고 도출된 요인의 합산평정점수를 구하였다. 다만 윤리성향과 Big-5 성격유형은 선행연구들을 통해 특정 요인이 구분된 척도로서 요인분석 없이 각 요인의 합산점수를 사용하였다. 또한 모든 요인들은 크론바흐 알파(Cronbach's α)를 이용하여 내적 일관성에 의한 측정도구의 신뢰도를 검증하였다.

2.3.1 윤리적 개념

Beebe&Clark(2006)는 높은 상대주의와 낮은 이상주의 윤리성향을 가진 해커들은 탈선적 해킹에 대해 용인적인 태도를 보인다고 보고했다. 본 연구에서는 위 결과에 기반 하여, 해커들의 윤리성향을 측정하기 위해 Forsyth(1980)가 제작한 윤리적 개념척도(Ethics Position Questionnaire)를 번안하여 사용했다. 본 척도는 총 20문항으로, 1-10번 문항까지는 이상주의(절대적 도덕규칙을 기준하여 판단을 내리는데 올바른 행위에 따른 올바른 결과를 믿는 주의)요인, 11-20번 문항까지는 상대주의(상황에 따른 유동적인 도덕규범을 따르며 절대적인 도덕기준이 없다고 믿는 주의)요인으로 구성되어 있다. 문항은 9점 척도(1=매우 그렇지 않다, 9=매우 그렇다)로 측정이 되었다. 주요인분석결과, 3문항이 제거되었으며, 이상주의 요인의 아이겐 값은 5.554에 전체변량 27.772%를 설명하였다. 문항 간 신뢰도는 .906이었다. 상대주의 요인의 아이겐 값은 4.860에 전체변량 24.299%를 설명하였으며, 문항 간 신뢰도는 .864이었다.

2.3.2 최적몰입경험

해커들의 최적몰입경험이 실제 해킹경험과 유의미한 정적상관관계를 갖는다는 우형진(2004)의 연구결과에 근거하여, 해커들의 최적몰입경험을 측정하기 위해, Jackson & Marsh(1996)[14]가 개발하고 우형진(2004)이 해킹상황에 맞게 수정한 최적경험상태 지수(Flow index)를 사용하였다. 총 20문항이 제시되었으며 5점 척도(1=매우 동의하지 않는다, 5=매우 동의한다)로 측정되었다. 주요인분석결과 모든 문항이 하나의 요인(uni- dimensionality)으로 나타났으며 아이겐 값 10.8에 전체변량의 54.1%를 설명하였다. 문항 간 신뢰도는 .954였다.

2.3.3 공격성

해커들의 공격적 기질 및 행위 요인이 타국에 대한 사이버테러 가능성을 예측하는 주요 변수임을 확인한 우형진(2004)의 연구에 근거하여, 해커들의 공격적인 기질과 반응을 알아보기 위해, Spielberger 외(1983)[15]가 제작하고 본 연구진이 번안한 공격적 기질과 반응(Angry Temperament and Angry Reaction)을 사용하였다. 척도는 공격적 성격과 반응, 행위에 대한 내용으로 구성되어 있으며, 4점 척도(1=거의 그렇지 않다, 4=거의 항상 그렇다)로 측정하였다. 이를 통해 해커의 심리구조 속에 존재하는 다양한 공격성과 반응에 대해 측정할 수 있었다. 주요인분석 결과 모든 문항이 하나의 요인으로 나타났으며, 아이겐 값 3.98에 전체변량의 39.8%를 설명하였다. 문항 간 신뢰도는 .818였다.

2.3.4 위험감수성향

Bachmann(2010)은 일반인 대조군에 비해 탈선적 해커집단이 위험과 스릴을 즐기는 높은 위험감수성을

가진다고 보고했다. 이에 근거하여, 해커들의 위험감수성향을 측정하기 위해 Knowles 외(1973)[16]가 제작하고 홍지연(2011)[17]이 번안한 위험감수 척도(Risk Taking Questionnaire)를 사용하였다. 위험감수 척도는 위험한 상황을 피하거나 접근하려는 의지에 대한 질문들로 구성되어 있으며, 20문항을 7점 척도(1=매우 그렇지 않다, 7=매우 그렇다)로 측정하였다. 주요인분석결과 모든 문항이 하나의 요인으로 묶였으며 아이겐 값 4.892에 전체변량의 32.615%를 설명하였다. 문항 간 신뢰도는 .861이었다.

2.3.5 Big-5 성격척도

해킹활동을 포함한 사이버범죄 집단은 일반인 통제군에 비해 특징적인 성격유형을 가지고 있다는 Rogers(2006)의 연구에 근거하여, 실제 해커들의 성격 특성을 알아보고자 Goldberg(1992)[18]가 정립한 Big-5 성격척도를 사용하였다. Big-5 성격척도는 개방성(openness to experience), 성실성(conscientiousness), 외향성(extraversion), 친화성(agreeableness), 정서불안정성(neuroticism)의 5개 요인을 측정하기 위한 35개의 문항들로 구성되어 있다. 요인 당 7문항씩 서로 반대되는 개념의 단어로 구성되어 있으며, 응답자는 상반되는 두 단어(예. 내향적 - 외향적) 중 자신의 성격과 가장 가깝다고 생각되는 단어에 점수를 주는 방식으로 응답하였다. 응답은 9점 척도로 측정되었다(1=왼쪽 단어에 매우 가까운, 5=어느 쪽도 아닌, 9=오른쪽 단어에 매우 가까운). 요인합산 점수가 높을수록 해당 요인의 성격에 가까운 것을 의미한다. 각 요인의 신뢰도 값은 외향성=.896, 성실성=.873, 개방성=.860, 친화성=.750, 정서불안정성=.884이었다.

2.3.6 해킹에 대한 태도

해킹에 대한 태도는 탈선적 해킹행위에 대한 해커들의 태도를 측정하기 위한 변수로서 해커들의 심리학적 특성들의 종속변수이자, 실제 해킹경험(해킹빈도, 해킹유형)과 해킹의도를 매개하는 변수로 사용이 되었다. 해킹에 대한 태도는 Beebe & Clark(2006)가 제작한 척도를 번안하여 사용하였다. '나는 허가 없이 정보 시스템에 접근하는 것에 큰 문제를 못 느낀다.' 외 4문항으로 구성되어있으며, 9점 척도(1=매우 그렇지 않다, 9=매우 그렇다)로 측정을 하였다. 총 점수가 높을수록 불법해킹활동에 대해 용인적인 태도를 가지고 있다는 것을 의미한다. 주요인분석결과 모든 문항이 하나의 요인으로 나타났으며 아이겐 값 2.581에 전체변량의 51.629%를 설명하였다. 문항 간 신뢰도는 .788이었다.

2.3.7 해킹 의도

해커들의 탈선적 해킹행위에 대한 의도(Willingness)를 측정하기 위해 Beebe & Clark(2006)이 제작한 척도를 번안하여 사용하였다. 척도의 각 문항은 해커들의 행동의지를 의미하는 문항들로 구성이 되어 있으며, 해커들이 선택하는 행동의도에 따라 해커들의 타입이 나뉘어진다.

(1) 나는 내 목적을 달성하기 위해서, 나의 능력과 지식을 가지고 허가되지 않은 정보시스템에 접근할 의향이 있다. (Blackhat)
(2) 나는 내 목적을 달성하기 위해서, 나의 능력과 지식을 가지고 허가되지 않은 정보시스템에 접근할 의향이 있었다. (Ex-blackhat)
(3) 나는 능력과 지식을 가지고 있지만, 이러한 기술들을 합법적으로 허가가 된 경우에만 사용할 의향이 있다. (Whitehat)
(4) 어느 문장도 해당사항이 없다. (Nohat)

위 척도는 실제 해킹행동이 아닌 응답자의 해킹행동에 대한 의도를 확인하는 데 사용되었다. 그러나 Fishbein과 Azjen(1975)[19]의 합리적 행위이론(Theory of Reasoned Action)에 따르면, 사람들의 행동을 직접적으로 결정하는 것은 행동을 하고자 하는 의도이며 이러한 의도에 영향을 미치는 것은 행동에 대한 태도라고 한다. 또한 연구에 있어 실제 행동을 관찰하는 것이 문제가 될 수 있는 특수한 경우에 의도가 미래 행동에 대한 충분한 예측타당도를 지니고 있다는 것을 인정하고 실제 행동에 대한 대용으로 측정하는 것이 널리 용인되고 있다(Trevino, 1992)[20]. 따라서 심리적 변수로 인한 해킹태도를 관찰하고, 결과적으로 해킹의도를 측정하는 것은 미래 탈선적인 해킹행동을 예측할 수 있을 뿐만 아니라, 해킹의도에 따른 해커들의 타입(Blackhat, Ex-blackhat, Whitehat, Nohat)을 예측하고 분류할 수 있는 근거가 된다.

2.3.8 해킹 경험(해킹빈도 & 해킹활동유형)

본 연구진은 해킹의도 이외에 추가적으로 실제 해킹경험을 측정하기 위한 종속변수를 사용했다. 해킹경험 척도는 해커들의 해킹빈도와 해킹유형을 확인할 수 있는 척도로써 우형진(2004)이 제작한 것을 사용하였다. 먼저 해킹빈도에 대해서는 '지난 한달 동안 사이버 공간에서 타인의 컴퓨터에 단순 침입한 횟수'와 '지난 한 달 동안 타인 소유의 사이버 정보 및 사이

표 1. 측정도구 항목
Table 1. List of research variables

Variables	Measurements		Properties
Independent Variables	Demographics		Individual's demographical information (Gender/Age/Education/Profession)
	Ethics Position Questionnaire (Forsyth, 1980)		Implemented to distinguish individual's ethical values. "Idealistic" types tend to strive for the righteous actions and believe such actions to be fair and noble, while "relativistic" types tend to believe there exists no comprehensive ethical measurement.
	Flow Index (Jackson & Marsh, 1996)		Implemented to measure the "optimal experience" that can be achieved contingent on individual's efficacy and the level of a given challenge. Higher score implies the higher level of optimal experience was achieved during the hacking activity.
	Angry Temperament and Angry reaction (Spielberger et al., 1983)		Implemented to measure one's hostility. This scale was used based on the terror management theory which states that when one's cultural values are threatened, one tends to react more angrily toward the origin of the threat. Higher score implies the higher angry temperament and aggressive reaction tendency.
	Risk Taking Questionnaire (Dahlbäck, 1990)		Scale that measures one's willingness in pursuing or avoiding risky situations. Higher score implies that individual's risk-taking tendency is higher.
	Big-5 Personality (Goldberg, 1992)		Scale that is used to explain individual differences through five distinctive factors. The five factors are openness to experience, conscientiousness, extraversion, agreeableness, and neuroticism. Higher score in each factor implies individual's stronger tendency in a given factor.
Mediator	Attitude: Ethicality of Hacking (Beebe & Clark, 2006)		Scale used to measure hackers' attitude toward deviant hacking activities (e.g. 1. I feel it is okay for a person to access information systems without authorization, with 4 items). Higher score means one is more tolerating of deviant hacking activities.
Dependent Variables	Hacking Experience (Woo, 2004)	Hacking Frequency	Measures hackers' hacking frequencies using the number of actual invasion or destruction of other's computer systems in past one month. Higher score implies the higher frequency of hacking activities.
		Categories of Hacking Activity	Utilized to distinguish types of hacking activities. Can be divided into three types: goal-oriented (targeted toward specific organizations such as governmental or religious institutes), non-goal oriented (hacking for fun or personal pleasure) and personally motivated (hacking is done for a personal gain). The total score can categorize a hacker into one of the three aforementioned types.
	Willingness to Hack (Beebe & Clark, 2006)		Survey designed to find one's willingness to attempt hacking (e.g. 1. I am willing to use my knowledge and skills to gain unauthorized access to information systems to serve my own goals, with 3 items). Subject is requested to select the most matching statement to one's own opinion, and depending on the selected statements one can be distinguished as one of the following types: Blackhat, Ex-blackhat, Whitehat, Nohat.

트 내용을 훼손한 횟수'를 각각 질문하였고 7점 척도(0=전혀 없다, 6=31회 이상)로 측정되었다. 문항 간 신뢰도는 .736이었다.

두 번째로 해킹활동유형은 다양한 해킹이유와 동기에 기반한 22가지의 해킹유형과 유형에 따른 활동정도를 확인할 수 있는 척도다. 각 항목들은 5점 척도(0=전혀 해킹한 경험이 없다, 4=매우 빈번히 한다)로 측정하였으며 주요인분석 결과, 6문항이 제거되었고 총 3개의 유형으로 분류되었다. 첫째, 목적지향형 해킹유형은 타국 정부나 회사의 웹사이트, 다른 종교의 웹사이트, 정보국의 웹사이트 등 특정 대상을 목표로 해킹을 수행한 유형을 말한다. 위 요인은 7개 항목으로 구성되었으며, 아이겐 값 5.559에 전체변량의 25.268%를 설명하였다. 문항 간 신뢰도는 .927이었다. 둘째, 비목적형 해킹활동유형은 특정한 목적 없이 해킹에 대한 관심이나 즐거움 추구를 위해 해킹을 수

행한 유형으로 재미를 위해, 호기심에, 심심해서 등이 해당된다. 위 요인은 6개 항목으로 구성되었으며 아이겐 값 4.554에 전체변량의 20.701%를 설명하였다. 문항 간 신뢰도는 .891이었다. 셋째, 사적동기형 해킹유형은 돈을 벌기 위해, 대학의 웹사이트 해킹, 개인 홈페이지 해킹 등 개인적인 목적성이 부여된 해킹활동 유형을 말한다. 위 요인은 6개 항목으로 구성되었으며 아이겐 값 4.297에 전체변량의 19.533%를 설명하였다. 문항 간 신뢰도는 .895이었다.

Ⅲ. 실험 결과

3.1 인구통계학적 결과

연구에 참여한 해커 91명의 인구통계학적 정보에 대해 빈도분석을 실시한 결과, 성별분포는 남성 91.2%, 여성 8.8%으로 남성에 편향되어 있는 것으로 나타났다. 나이별로는 20-25세의 경우에 73.6%, 19세 이하는 14.3%, 26-30세가 6.6% 순으로 나타났다. 최종학력의 경우에는 대학교 재학이나 졸업이 86.8%, 고등학교 재학이나 졸업이 9.9% 순으로 나타났다. 전문성의 경우에는 일반컴퓨터 사용자가 80.2%, 컴퓨터 전문가 19.8%로 나타났다(표 2).

3.2 심리학적 특성이 해킹태도에 미치는 영향

다양한 심리학적 특성이 해킹에 대한 태도에 미치는 영향을 알아보기에 앞서, 인구통계학적 특성이 심리변수에 주는 영향력을 측정하기 위해 심리학적 특성에 대해 다중회귀 분석(multiple regression analysis)을 실시하였다. 인구통계학적 특성은 해킹에 대한 태도에는 직접적인 영향을 주지는 않았으나, 일부 심리학적 특성에 영향을 미쳤다(나이→상대주의 β=-.460 p<.001, 전문성→최적몰입경험 β=.341 p<.01, 최종학력→위험감수성 β=-.267 p<.05, 전문성→개방성 β=.267 p<.05).

표 2. 피험자들의 인구통계학적 정보 결과
Table 2. Sample Descriptive Statistics

		Total	Percentage
Gender	Male	83	(91.2)
	Female	8	(8.8)
Age	Under 19	13	(14.3)
	20-25	67	(73.6)
	26-30	6	(6.6)
	31-35	3	(3.3)
	36-40	2	(2.2)
Level of Education	Not Completed High School	2	(2.2)
	Completed High School	9	(9.9)
	Undergraduate degree	79	(86.8)
	Graduate degree	1	(1.1)
Profession	Computer user	73	(80.2)
	Computer Professional	18	(19.8)
	Total	91	(100.0)

이 후 심리학적 특성들이 해킹태도에 미치는 영향에 대하여 위계적 회귀분석(hierarchial regression analysis)을 실시하였다. 먼저 인구통계학적 정보를 통제변수로 성별, 나이, 학력, 전문성을 투입하였으며, 설명력은 .2%로 낮게 나타났다. 분석결과, 심리변수들 중 최적경험의 표준화 베타 값(β)이 .275로 나타나 유의미한 정적영향을 미쳤다(p<.05). 또한 윤리성향 중 이상주의가 해킹태도에 미치는 영향은 표준화 베타 값(β)이 -.386로 나타나 유의미한 부적영향을 미쳤다(p<.01). Big-5 성격 중 정서불안정성의 표준화 베타 값(β)은 .290로 근사적으로 유의미한(marginally significant) 영향을 끼쳤다(p=.051). 회귀식의 설명력은 28%로 나타났다.

위 결과는 범법적 해킹에 관여한다고 알려진 해커들의 다양한 심리변수들 중 높은 최적경험과 윤리성향 중 낮은 이상주의 성향을 가진 해커들이 탈선적인 해킹태도에 있어 용인적인 태도를 가진다는 것을 의미한다.

3.3 해킹에 대한 태도가 해킹경험에 미치는 영향

해킹태도가 해킹활동유형에 미치는 영향에 대하여 위계적 회귀분석을 실시하였다. 해킹태도는 실제 해킹활동유형에 유의미한 영향을 미치는 것으로 나타났다. 해킹유형 요인 중 목적지향형 해킹유형에 대한 해킹태도의 표준화 베타 값(β)이 0.357로 나타나 정적으로 유의미한 영향을 미쳤다(p<.01). 회귀식의 설명력은 16%로 나타났다. 또한 비목적 지향형 해킹유형에 대한 해킹태도의 표준화 베타 값(β)이 0.309로 나타나 정적으로 유의미한 영향을 미쳤다(p<.01). 회귀식의 설명력은 34%로 나타났다. 하지만, 사적동기형 해킹유형의 경우에는 해킹태도가 유의미한 영향을 미치지 않았다(β=0.357, p>.05). 회귀식의 설명력은 9%로 나타났다. 이러한 결과는 해킹태도 점수가 높을수록(탈선적 해킹에 용인적인 태도를 가질수록), 목적지향형, 비목적형 해킹활동도 높아지는 것을 알 수 있으며, 사적동기형 해킹유형과는 관련성이 없다는 것을 알 수 있다.

해킹태도가 해킹빈도에 미치는 영향은 표준화 베타 값(β)이 -0.265로 나타나 부적인 영향이 나타났으나, 통계적으로 유의미한 영향은 미치지 않았다(p=.224).

회귀식의 설명력은 66%로 나타났다. 이는 해킹에 대한 태도가 해킹빈도에는 큰 영향을 미치지 않는다는 것을 의미한다.

3.4 해킹에 대한 태도가 해킹의도에 미치는 영향

해킹에 대한 태도가 해킹의도(Blackhat, Ex-Blackhat , Whitehat, Nohat)에 미치는 영향력을 알아보기 위해 다항 로지스틱 회귀분석(Multinomial logistic regression)을 실시하였다.

Nohat(4.어느 문장도 해당사항이 없다.)을 참조변수로 기준하여, 각 해킹의도에 대한 해킹태도의 영향을 검증한 결과, Blackhat(1. 나는 내 목적을 달성하기 위해서, 나의 능력과 지식을 가지고 허가되지 않은 정보시스템에 접근할 의향이 있다.)에서 해킹태도가 유의미한 수준으로 정적 영향을 보였다(β추정값=.539, p<.05). 해킹태도는 해킹의도 변량의 약 19%를 설명했다(Cox&Snell=.192, Nagelkerke=.211). 이러한 결과는 해킹태도 점수가 높은 경우, 즉 탈선적 해킹에 용인적인 태도를 지닐수록, 상대적으로 해킹의도 중 Blackhat을 선택할 가능성이 높아짐을 의미한다. 하지만 나머지 해킹의도(Ex-blackhat, Whitehat)에 대해서는 부적 영향력이 나타나긴 했지만 유의미한 차이가 나타나지 않았다(표 3). 추가적으로 다항로지스틱 회귀식의 설명력을 높이기 위하여, 인구통계학적 정보를 해킹태도와 함께 독립변수로 해킹의도에 대한 영향력을 알아보았다. 그 결과 변량의 약 32%를 설명했으며(Cox&Snell=.322, Nagelkerke =.354), 인구통계학적 정보는 해킹의도에 유의미한 영향을 미치지 않았다. 오직 해킹태도만이 해킹의도에 유의미한 영향을 미쳤는데, 결과의 방향성은 이전과 동일하게 나타났다(해킹태도→Blackhat β추정값=.605, p<.05).

본 연구의 목표 중 하나는 연구진이 보완한 연구모델로 해킹의도에 따른 해킹타입, 그 중에서도 사이버범죄에 가담할 가능성이 높은 Blackhat타입을 분류하는 것이다. 따라서 Blackhat을 가장 잘 판별해주는 함수를 계산하기 위해 인구통계학적 정보와 해킹에 대한 태도를 독립변수로 하여 해킹의도에 대한 판별분석(Discriminant analysis)을 실시하였다. 정준판별함수는 다음 식(1)과 같다.

$$y = -1.821 + .554(\text{Gender}) - .405(\text{Age}) + .277(\text{Education}) - .254(\text{Expertise}) + .658(\text{Attitudes}) \quad (1)$$

위 식은 판별함수와 변수들 간의 상관관계 계수를 나타낸 것으로서 계수 값이 클수록 판별함수에 영향을 크게 미친다. 판별함수에 가장 큰 영향을 미치는 변수는 해킹태도였다. 분석결과, Blackhat을 올바로 분류할 확률은 66.7%, 그 외 해커타입은 77.1%로 인구통계학적 정보와 해킹에 대한 태도만으로 해킹의도를 74.7% 정확도로 분류할 수 있음을 보였다.

표 3. 해킹에 대한 태도가 해킹의도에 미치는 영향 다항로지스틱 회귀분석 결과
Table 3. Multinominal logistic regression result

Willingness to Hack		β estimate value	Wald	p	odd ratio
Blackhat	fragment	-1.786	5.213	.022	
	Attitude of Hack	.539*	6.467	.011	1.714
Ex-blackhat	fragment	-.933	.938	.058	
	Attitude of Hack	-.104	.098	.754	.901
Whitehat	fragment	1.315	5.379	.444	
	Attitude of Hack	-.220	1.283	.257	.802

Nohat as Reference

Ⅳ. 결 론

탈선적 해킹에 영향을 주는 다양한 심리변수들 중 탈선적 해킹태도에 가장 큰 영향을 차지하는 심리변수는 해커들의 낮은 '이상주의적 윤리성향'과 높은 '최적몰입경험'임을 밝혀냈다. Big-5 성격유형 중 높은 '정서불안정성'은 탈선적 해킹태도에 근사적으로 유의미한 영향을 주었다. 또한 도출된 해킹태도 점수는 목적지향적 해킹활용유형과 비목적형 해킹활동유형을 유의미하게 예측하였으며 탈선적 해킹의도 또한 유의미하게 예측하였다. 추가적으로 의도에 따라 구분된 해커 타입 중 실제 해킹범죄에 관여할 가능성이 있는 Blackhat 타입의 해커들을 높은 확률로 분류할 수 있었다.

본 연구에서 낮은 이상주의적 윤리성향과 해킹태도와의 관련성은 Beebe & Clark(2006)의 기존 결과를 뒷받침하는 결과이다. 즉, 절대적 도덕규칙을 기준하여 올바른 행위를 추구하는 이상주의적 윤리성향이 상대적으로 낮은 해커들이 탈선적 해킹에 용인적인 태도를 가졌다. 또한 높은 '최적몰입경험'과 해킹태도와의 관련성은 해커가 해킹행동을 하면서 느끼는 최적몰입경험이 높을수록, 탈선적 해킹에 대한 태도가 용인적이고, 이러한 태도가 해킹활동과 해킹의도에 영향을 준다고 해석될 수 있으며, 이는 우형진(2004)의

연구결과와 그 맥락을 같이 한다. 또한 탈선적 해킹태도와 정서불안정성 성격유형에 대한 결과는, 정서불안정성 성격유형이 범법적 행동과 관련이 있다는 Eysenck(1985)[21]의 연구결과를 지지하는 것이다.

기존의 선행연구들은 다면적인 인간의 심리 중 하나의 특성에만 초점을 맞추었기 때문에 어떠한 심리적 특성이 탈선적 해킹과 가장 연관되어 있는지는 알기 어려웠다. 특히 Beebe & Clark (2006)의 기존 연구모델은 해커들의 윤리성향에 대한 심리적 특성만을 보았다. 그러나 본 연구는 탈선적 해킹태도에 관여하는 다양한 심리변인을 고려한 탐색적 연구로서 해킹태도에 유의미하게 영향을 끼치는 추가적인 심리변인을 확인하였다. 또한 종속변인으로 해킹의도 뿐 아니라 해커들의 실제 해킹활동경험을 측정하여 보다 종합적인 예측모델을 수립할 수 있었다(그림 4).

본 연구는 대다수의 기술적 접근에 그친 연구가 아닌 심리학적 접근을 활용한 해커연구라는 점에서 차별성을 지닌다. 이는 매년 대두되고 있는 다양한 사이버범죄에서 심리변수에 근거한 해커들의 프로필을 발전시킬 수 있는 가능성을 제시하고, 차후 신경과학 및 심리생리측정 방법론을 도입한 연구의 기반이 될 수 있다.

그러나 신분노출을 극도로 꺼리는 해커들의 특성상 많은 수의 해커들을 모집하지 못한 점, 또한 피험자가 주로 해킹기술을 보유한 대학생들이라는 점에서 한계점을 지니며, 추후 확장적인 연구가 필요할 것으로 보인다.

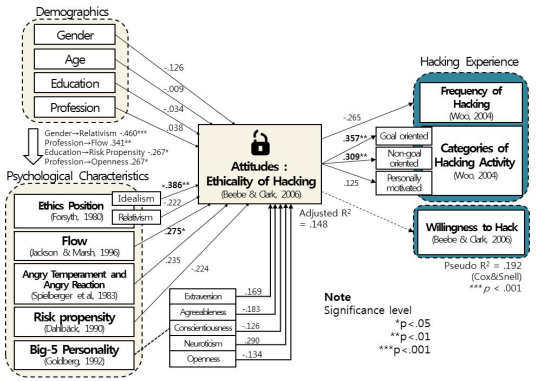


그림 3. 회귀분석 결과
Fig. 3. Regression result

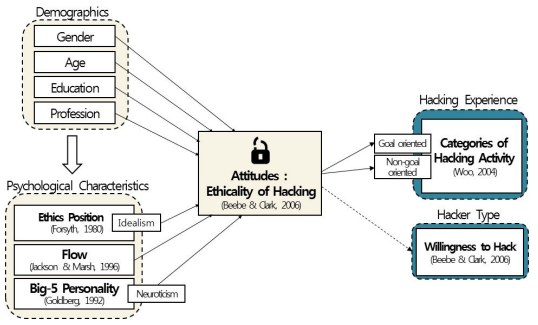


그림 4. 본 연구에서 도출된 종합적 해킹예측모델
Fig. 4. A comprehensive prediction model derived from the result

References

[1] F. Xu, B. Qi, and H. K. Lo, "Experimental demonstration of phase-remapping attack in a practical quantum key distribution system," *New J. Physics*, vol. 12, no. 11, pp. 14-28, Nov. 2010.

[2] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," *Nature Photonics*, vol. 4, no. 10, pp. 686-689, Aug. 2010.

[3] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, "Full-field implementation of a perfect eavesdropper on a quantum cryptography system," *Nature Commun.*, vol. 2, no. 349, Jun. 2011.

[4] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, and G. Leuchs, "Device calibration impacts security of quantum key distribution," *Physical Rev. Lett.*, vol. 107, no. 11, pp. 110501(1-5), Sept. 2011.

[5] Y. Liu, Y. Cao, M. Curty, S. K. Liao, J. Wang, K. Cui, and H. F. Zhang, "Experimental unconditionally secure bit commitment," *Physical Rev. Lett.*, vol. 112, no. 1, pp. 010504(1-5), Jan. 2014.

[6] M. Rogers, *Preliminary findings: understanding criminal computer behavior: a personality trait and moral choice analysis*, Retrieved June, 27, 2009, from http://homes.cerias.purdue.edu/~mkr/CPA.doc

[7] G. Rose, H. Khoo, and D. W. Straub, "Current technological impediments to business-to-consumer electronic commerce," *Commun. AIS*

(CAIS), vol. 1, no. 16, Jun. 1999.

[8] K. Buyens, B. D. Win, and W. Joosen, "Empirical and statistical analysis of risk analysis-driven techniques for threat management," in *Proc. IEEE ARES 2007,* pp. 1034-1041, Vienna, Austria, Apr. 2007.

[9] N. L. Beebe and J. Guynes, "A model for predicting hacker behavior," in *Proc. AMCIS 2006*, vol. 409, Acapulco, Mexico, Dec. 2006.

[10] D. R. Forsyth, "A taxonomy of ethical ideologies," *J. Personality and Social Psychology*, vol. 39, no. 1, pp. 175-184, Jul. 1980.

[11] H. J. Woo, "A study on the relationship between hackers' psychological variables and hacking activities," *Korean J. Journalism & Commun. Stud.*, vol. 48, no. 3, pp. 90-115, Jun. 2004.

[12] M. Bachmann, "The risk propensity and rationality of computer hackers," *The Int. J. Cyber Criminology*, vol. 4, no. 1-2, pp. 643-656, 2010.

[13] M. Rogers, N. D. Smoak, and J. Liu, "Self-reported deviant computer behavior: a big-5, moral choice, and manipulative exploitive behavior analysis," Deviant Behavior, vol. 27, no. 3, pp. 245-268, 2006.

[14] S. A. Jackson and H. W. Marsh, "Development and validation of a scale to measure optimal experience: The flow state scale," *J. Sport and Exercise Psychology*, vol. 18, no. 1, pp. 17-35, Dec. 1996.

[15] C. D. Spielberger, G. Jacobs, S. Russell, and R. S. Crane, "Assessment of anger: The state-trait anger scale," in *Advances in Personality Assessment*, vol. 2, pp. 161-189, Lawrence Erlbaum Associates, 1983.

[16] E. S. Knowles, H. S. Cutter, D. H. Walsh, and N. A. Casey, "Risk-taking as a personality trait," *Social Behavior and Personality: an Int. J.*, vol. 1, no. 2, pp. 123-136, Jan. 1973.

[17] J. Y. Hong and Y. H. Cho, "A study the impacts of gamblers' risk taking and maladaptive beliefs on the gambling behavior," *J. Tourism Sci.*, vol. 35, no. 8, pp. 367-388, Oct. 2011.

[18] L. R. Goldberg, "The development of markers for the Big-Five factor structure," *Psychological assessment*, vol. 4, no. 1, pp. 26-42, Mar. 1992.

[19] M. Fishbein and I. Azjen, *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research*, Addison-Wesley, 1975.

[20] L. K. Trevino, "Moral reasoning and business ethics: Implications for research, education and management," *J. Business Ethics*, vol. 11, no. 5, pp. 445-464, May 1992.

[21] H. J. Eysenck and M. W. Eysenck, *Personality and Individual Differences*, Plenum Press, 1985.

박 찬 현 (Chan Hyun Park)

2014년 2월 : 울산대학교 미생물유전공학과 학사

2014년 3월~현재 : 고려대학교 심리학과 석사과정

<관심분야> 해커심리학, 가상현실, 다감각통합

송 인 욱 (In Uk Song)

2015년 2월 : 고려대학교 심리학과 학사

2015년 3월~현재 : 고려대학교 심리학과 석사과정

<관심분야> 범죄심리학, 신경법학, 해커심리학

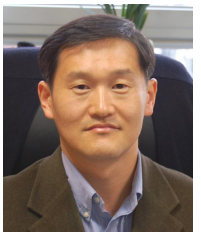
김 민 지 (Min Ji Kim)

2014년 8월 : 경희대학교 언론정보학과 학사
2014년 9월~현재 : 고려대학교 심리학과 석사과정
<관심분야> 인지통제, 정서, 양가감정

장 은 희 (Eun Hee Chang)

2011년 2월 : 고려대학교 화학화, 심리학과 학사
2013년 9월 : 고려대학교 심리학과 석사
2015년 9월~현재 : 고려대학교 심리학과 박사과정
<관심분야> 다감각통합, 가상현실, 해커심리학

허 준 (Jun Heo)



1989년 2월 : 서울대학교 전기공학과 학사
1991년 2월 : 서울대학교 전기공학과 석사
2002년 8월 : 미국 USC 전자공학과 박사
2003년 3월~2007년 2월 : 건국대학교 전자공학부 조교수
2007년 3월~2012년 9월 : 고려대학교 전기전자전파공학부 부교수
2012년 10월~현재 : 고려대학교 전기전자전파공학부 정교수
<관심분야> 통신시스템, 채널코딩, MIMO

김 현 택 (Hyun Taek Kim)

1985년 : 고려대학교 심리학과 학사
1987년 : 고려대학교 심리학과 석사
1991년 : 고려대학교 심리학과 박사
1998년 : University of Texas, Medical school in Galveston 방문교수
1992년~2001년 : 고려대학교 심리학과 부교수
2001년~현재 : 고려대학교 심리학과 정교수
<관심분야> 범죄심리학, 가상현실, 인지와 정서의 뇌기전