Information Systems Review
Vol. 19, No. 3 September 2017 http://dx.doi.org/10.14329/isr.2017.19.3.201

취약점 연구동기가 취약점마켓 이용의도에 어떠한 영향을 미치는가?

How Vulnerability Research Motives Influence the Intention to Use the Vulnerability Market?

김 형 열 (Hyeong-Yeol Kim) 주식회사 에이쓰리시큐리티
김 태 성 (Tae-Sung Kim) 충북대학교 경영정보학과, 교신저자

요 약

정보자산에 심각한 피해를 입힐 수 있는 보안 취약점 정보는 상품으로서 가치를 갖게 되었으며 취약점마켓이 형성되었다. 이러한 보안 취약점 정보는 심각성과 중요도에 따라 취약점마켓에서 수백 달러부터 수십만 달러로 거래되고 있으며 종류와 범위는 다양해지고 있다. 본 연구는 취약점마켓과 해커에 관한 선행연구를 토대로 보안 연구자의 취약점 연구동기와 취약점마켓 이용의도에 영향을 미치는 요인에 대한 실증 분석을 실시하였다. 연구결과는 다음과 같다. 첫째, 취약점 연구 자기효능감은 몰입, 화이트마켓 이용의도, 블랙마켓 이용의도에 유의한 영향을 미치고 인지된 이익에는 유의한 영향을 미치지 않았다. 둘째, 몰입은 인지된 이익과 블랙마켓 이용의도에 유의한 영향을 미쳤으나 화이트마켓 이용의도에는 유의한 영향을 미치지 않았다. 셋째, 인지된 이익은 화이트마켓 이용의도와 블랙마켓 이용의도에 모두 유의한 영향을 미쳤다. 넷째, 취약점 연구 자기효능감은 몰입을 매개로 인지된 이익에 유의한 영향을 미쳤다. 다섯째, 몰입은 인지된 이익을 매개로 화이트마켓 이용의도와 블랙마켓 이용의도에 모두 유의한 영향을 미쳤다. 본 연구는 취약점 연구경험이 있는 보안 연구자의 행동 예측에 활용될 수 있을 것이다.

키워드 : 보안 연구자, 취약점마켓, 취약점 연구 자기효능감, 몰입, 인지된 이익, 취약점마켓 이용의도

Ⅰ. 서 론

정보기술의 발전으로 경제와 사회에서 정보시스템의 중요성은 증가하고 있으며 기업에서는 전자상거래, 고객 서비스, 물품 조달, 직원 관리 등을 위하여 소프트웨어 및 웹 사이트와 같은 정보시스템을 이용하고 있다. 취약점(Vulnerability)은 침투하기 위한 공격로를 공격자에게 제공할 수 있는 소프트웨어, 하드웨어, 절차, 사람에 대한 약점이다(Ablon *et al.*, 2014). 보안 취약점을 통해 인가되지 않은 공격자에 의해 기업의 정보시스템 데이터는 침범, 파괴, 조작, 유출 등과 같은 피해를 입을 수 있다. Bambauer and Day(2010)에 따르

† 본 연구는 과학기술정보통신부 및 한국인터넷진흥원의 "고용계약형 정보보호 석사과정 지원사업"의 연구결과로 수행되었음(과제번호 H2101-16-1001). 이 논문은 2015년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임(NRF-2015S1A5A2A01009763).

면 정보보호침해의 75%는 소프트웨어의 결함으로 나타났다. 이에 기업에서는 정보시스템 자산의 위협을 줄이기 위한 다양한 시도를 하고 있다.

이러한 환경에서 소프트웨어 취약점 정보는 상품으로서 가치를 지니게 되었고 취약점 공개와 함께 취약점마켓이 이슈가 되었으며 해커들 사이에서 소프트웨어 취약점 정보가 거래되고 있다(Ablon *et al*., 2014). 소프트웨어의 취약점 정보를 사고파는 시장을 통칭하여 취약점마켓(Vulnerability Market)이라고 한다(Böhme, 2006). 취약점마켓의 종류는 거래의 합법성과 목적에 따라 화이트마켓, 블랙마켓, 그레이마켓으로 구분된다. Fobos(2012)에 따르면 Microsoft, Google, Oracle, Adobe와 같은 주요 소프트웨어 기업의 제품에 대한 제로데이 취약점(Zero-Day Vulnerability)이 그레이마켓과 블랙마켓에서 비싼 가격에 거래되고 있다. 국내에는 삼성과 네이버와 같은 일부 대기업을 제외한 대부분의 기업은 자사 제품의 취약점 신고가 제보되어도 이를 보상할 능력이 없다. 이런 이유로 국내에서는 한국인터넷진흥원(Korea Internet and Security Agency, KISA)에서 'S/W 취약점 신고 포상제도'를 실시하고 있다(한국인터넷진흥원, 2016). 취약점마켓을 통하여 기대하는 점은 다음과 같다. 취약점마켓은 보안 취약점 연구자 개인에게 합법적인 연구공간을 제공함으로써 범죄 가능성이 낮아지고 합법적이고 정당한 보상 및 명성을 얻을 수 있는 기회의 장이 될 수 있다. 또한 기업에서는 자체적으로 해결할 수 없는 보안 취약점 문제를 해결하고 소비자에게 기업의 보안 신뢰도를 높일 수 있는 수단으로 취약점마켓을 이용할 수 있다(Elgamal *et al*., 2013; Finifter *et al*., 2013).

이에 보안 취약점 정보를 발견할 수 있는 역량을 지닌 보안 연구자의 역할이 중요하며 이들의 행동에 대한 연구가 필요하다. 해외에서는 2010년대 초부터 취약점마켓에 대한 활발한 연구가 진행되었다(Algarni *et al*., 2013, 2014; Arora *et al*., 2010; Finifter *et al*., 2013; Zaho *et al*., 2014, 2015). 이후 취약점마켓에서 거래되는 취약점의 종류 및 트렌드 그리고 취약점마켓 참여자에 대한 인터뷰를 통하여 취약점마켓 참여 동기를 묻고 서비스에 반영하는 수준으로 진행되었다(Algarni *et al*., 2014). 반면, 국내의 취약점 연구는 취약점 발견과 관련한 기술적 연구에 집중된 반면 취약점의 수요예측 및 활용방안에 관한 연구는 제한적이다(김민정, 유진호, 2014).

본 연구에서는 향후 취약점마켓에 참여할 가능성이 있는 일정 수준에 도달한 보안 연구자들을 대상으로 실증연구를 실시하였다. 보안 연구자들의 행동을 탐구하는 연구는 그 자체로서 중요한 의미를 지닐 뿐만 아니라 취약점마켓 도입과 관련하여 실무적인 의의를 가질 것으로 기대한다.

Ⅱ. 이론적 배경

2.1 취약점마켓

2.1.1 취약점마켓 현황 및 종류

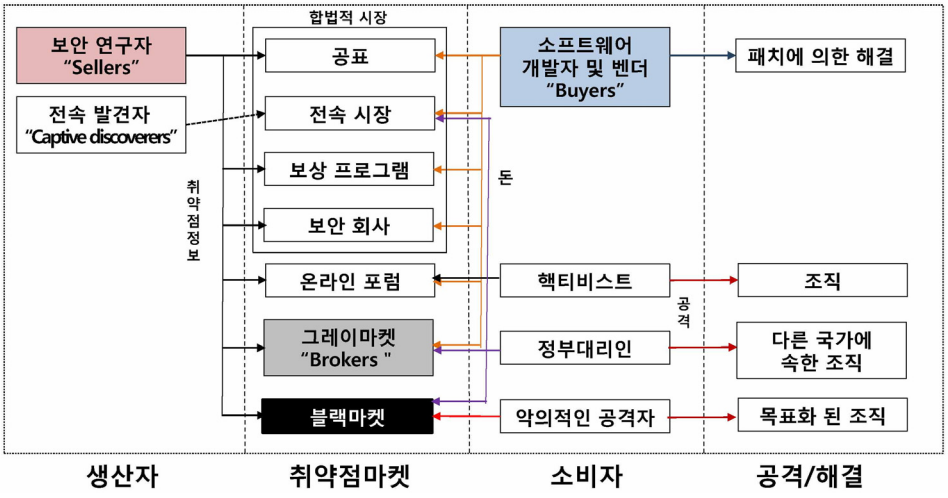
정보통신 기술이 고도화되면서 산업 전반에 정보시스템(Information System, IS)의 가치가 높아졌으며, 이를 침해할 수 있는 보안 취약점에 대한 중요성도 증가하고 있다. 특히 세계 최대 인터넷 검색 서비스 회사인 구글(Google)에서는 소프트웨어에 대한 잠재적인 취약점의 수를 줄이기 위하여 코드 리뷰(Code Review), 침투 테스팅(Penetration Testing), 정적 및 동적 분석 툴 사용(Use of Dynamic and Static Analysis Tools), 취약점 보상 프로그램(Vulnerability Rewards Program)을 이용하는 등의 노력을 하고 있다(Finifiter *et al*., 2012). 또한 Facebook, Apple, Oracle과 같은 소프트웨어 벤더들도 취약점을 줄이기 위한 방법으로 취약점 정보를 구매하고 있다. 정보보안 관련 연구자 워크샵인 NSPW(New Security Paradigms Workshop)에서도 기업의 중요 자산인 정보시스템에 위협을 줄 수 있는 취약점 정보의 거래 및 활용에 대한 윤리적 및 법적 이슈를 논의하였다(Elgamal *et al*., 2013).

취약점마켓을 알기 위해선 취약점(Vulnerability)

에 대한 이해가 필요하다. 비영리 공공 연구 기관인 RAND 연구소(RAND Corporation)는 취약점을 공격자가 악용할 수 있는 통로를 제공할 수 있는 소프트웨어, 하드웨어, 절차적 또는 인간의 약점으로 정의하였다(Ablon *et al*., 2014). 한국인터넷진흥원에 따르면 보안취약점을 소프트웨어 실행시점에 보안약점이 원인이 되어 발생하는 실제적인 위협이라고 정의하였다(한국인터넷진흥원, 2016). 이러한 보안 취약점 정보는 기업의 정보시스템을 공격하거나 방어하는 당사자에게 가치 있는 자산이 되었으며 취약점마켓이란 개념이 등장하였다(Böhme, 2006). 취약점마켓(Vulnerability Market)이란 소프트웨어의 취약점 정보를 거래하는 시장을 뜻한다. 취약점마켓에서는 보안 연구자 또는 해커들이 자신의 능력으로 발견한 취약점 정보를 팔 수 있는 다양한 환경을 제공한다. 취약점마켓의 종류는 거래의 합법성과 목적에 따라 화이트마켓, 블랙마켓, 그레이마켓으로 구분된다(<그림 1> 참조).

Algarni *et al*.(2014)에 따르면 취약점마켓에는 책임 있는 기관에 공개 절차를 거치는 '공표', 조직의 소프트웨어 개발 조직의 취약점 탐지 부서 또는 그 조직의 계약에 따라 일하는 '전속 시장', 쉽고 합법적인 방식으로 직접 벤더에 결과물을 팔 수 있는 '보상 프로그램', 취약점 발견을 통해 고객에게 보다 높은 수준의 안전을 제공하는 '보안 회사'와 같은 합법적인 시장, 취약점과 익스플로잇에 대한 정보를 교환할 수 있는 '온라인 포럼', 어느 정도 법적으로 보장된 오픈 마켓에서 개인이나 국가 단위로 취약점 구매자와 판매자들의 가격에 협상에 따라 취약점이 거래되는 '취약점 브로커', 사이버 범죄자, 테러리스트 또는 정부기관이 합법적이지 않은 공간에서 취약점을 거래하는 '취약점 암시장'으로 구성된다.

화이트마켓(White Market)이란 소프트웨어 개발자 및 벤더가 보안 연구자에게 취약점 보고서에 대한 보상금을 지급하는 시장으로 다양한 정의가 있다(Ablon *et al*., 2014; Fidler, 2014; HP, 2014). HP(2014)에 따르면 화이트마켓은 버그 바운티 프로그램, 해킹 콘테스트 그리고 직접 벤더와의 커뮤니케이션을 통해 책임 있는 공개에 대한 기회를 제공하는 것으로 정의하였다. Fidler(2014)는 화이트마켓을 네트워크 보안 솔루션을 제공하는 티핑포인트(Tipping Point)와 같이 제로데이 취약점 판매자, 소프트웨어 벤더, 제3자 취약점 정보센터 사이에서 법적 상호거래를 포괄하는 것이라고 정의하였다. 화이트마켓은 세 가지로 구분된다. 자사



〈그림 1〉 취약점마켓 메커니즘

제품의 취약점 정보에 대해 소프트웨어 벤더가 보상을 제공하는 프로그램(Company Sponsored Bounty Program), 문제를 해결하는 소프트웨어 개발자와 함께 일함으로써 제3자에게 판매하는 제3자 구매 프로그램(Third-Party Purchasing Program), 정부 공개 프로그램(Government Disclosure Program)이 있다(Ablon *et al*., 2014; Fidler, 2014).

블랙마켓(Black Market)이란 악의적인 의도로 해킹 툴, 해킹 서비스, 해킹의 과실을 거래하는 시장이다(Ablon *et al*., 2014). HP(2014)에 따르면 블랙마켓에서는 소프트웨어 취약점 결함에 대해 높은 가격을 제시한 입찰자에게 판매되며, 이러한 취약점 결함을 민간이나 공적인 개인이나 그룹에 침투하면서 악용할 수 있다고 한다. Fidler(2014)는 블랙마켓을 구매자 또는 판매자가 범죄적으로 서로 거래하는 공간이라 정의하였다. 예를 들면, 보안 취약점을 찾는 능력을 가진 자와 범죄 조직사이의 거래를 말하는 것이다. 이러한 블랙마켓은 범죄조직, 개별적인 불법 판매자 또는 구축된 블랙마켓 사이트로부터 취약점을 구매하는 정부 대리인(Government Agency)으로 구성된다.

그레이마켓(Gray Market)이란 취약점과 익스플로잇의 거래, 발견 및 개발 그 자체로는 불법이 아니지만 문제를 일으킬 수 있는 시장이다(Ablon *et al*., 2014). HP(2014)에 따르면 그레이마켓은 제로데이 마켓 내에서 주로 합법적 회사(정부)가 법적 회색 지대에서 운영하는 것이다. 그레이마켓에서는 정부와 같은 법적으로 힘 있는 대리인이 익스플로잇을 구매하기 때문에 이러한 행위들은 전 세계의 시스템 방어체계의 생명주기를 복잡하게 만들 수 있다(Ablon *et al*., 2014).

2.1.2 취약점마켓 연구 동향

2000년대 초, 인터넷 보급이 활성화 되면서 정보 시스템에 직접적인 위협을 줄 수 있는 취약점 공개에 대한 시장의 영향력 및 경제적 효과에 대한 연구 및 논의가 진행되었다(Böhme, 2006; Cambell *et al*., 2003; Nizovtsev *et al*., 2005; Telang and Sunil, 2005). 정보보호침해의 경제적 효과에 대하여 주식시장에서 시장 참여자는 정보보호침해 공표에 대하여 부정적이고 차별적인 반응을 보인 연구 결과가 있다(Cambell *et al*., 2003). 즉, 주식 시장 참여자는 기밀 데이터가 수반된 침해에 대하여 부정적인 반응을 보였고, 기밀 데이터를 수반하지 않은 침해에 대하여는 아무런 반응을 보이지 않는다는 것을 보였다. Nizovtsev *et al*.(2005)은 게임 이론 관점에서 접근하여 합리적 손실-대리인 최소화 게임에 대한 균형 전략을 보여주었다. 시장에서 취약점 공개 기회가 존재하면 예상된 손실을 감소시키고 사회 복지(Social Wellbeing)를 향상시킬 수 있다고 하였다. 금융 시장을 대상으로 사건 연구 방법을 사용하여 소프트웨어 취약점 공개의 영향을 분석한 결과, 취약점 공개는 소프트웨어 벤더의 시장가치에 상당히 부정적인 변화를 이끄는 것으로 나타났다(Telang and Sunil, 2005). 이러한 흐름 속에서 외부의 보안 연구자들을 대상으로 취약점 정보를 직접 거래하는 취약점마켓이란 용어와 개념이 등장하였다(Böhme, 2006). 국내의 취약점 정보활용 관련 연구는 소프트웨어 취약점으로 인한 손실비용을 전염병 확산 모델을 적용하여 수리적 방법으로 취약점 손실 비용을 추정한 연구가 있다(김민정, 유진호, 2014).

보안 취약점 정보의 거래가 민간 대기업 벤더(Google, Microsoft, Oracle, Facebook 등)와 취약점 보상 프로그램을 중심으로 활성화되면서 취약점 마켓을 구성하는 취약점 발견자, 취약점마켓, 취약점 구매자 등에 대한 연구가 진행되었다(Algarni *et al*., 2013, 2014; Arora *et al*., 2010; Finifter *et al*., 2013; Zaho *et al*., 2014, 2015). Arora *et al*.(2010)는 소프트웨어 벤더의 패치 배포(patch release)와 취약점 공개(vulnerability disclosure)의 영향에 관하여 분석하였다. 취약점 공개가 패치 배포를 가속화하고, 큰 벤더의 패치 배포는 작은 벤더보다 빠르고, 심각한 취약점에 대하여 벤더가 배포한 패치는 더 빨리 설치되고, 벤더는 CERT에 공개된 취약점에 대하여 더 빨리 응답하고, 오픈 소스 벤더가 상용

소프트웨어 벤더보다 더 빨리 설치된다는 것을 보였다. Algarni *et al.*(2013)은 가장 성공적인 취약점 발견자를 대상으로 인터뷰하여 성공적인 취약점 발견과 취약점마켓에 대한 참여 동기를 일으키거나 참여가 가능하게 하는 요인들을 도출하였다. 성공적인 취약점 발견자는 소프트웨어 보안에 상당한 전문지식을 갖고 있으며 이들 대부분이 소프트웨어 보안 조직에 속해있고, 금전적 보상에 상당한 동기를 갖고 있음을 확인하였다. Finifter *et al.*(2013)은 구글 크롬과 모질라 파이어폭스의 취약점 보상 프로그램의 지난 3년간의 데이터를 수집한 후에 비용, 이익, 인기도, 효용성과 같은 측정도구를 이용하여 취약점 보상 프로그램의 비용 효과성을 평가하였다. 취약점을 발견할 수 있는 보안 전문가들은 기발한 버그나 특별한 이벤트를 찾아 그에 상응하는 보상금을 받길 원하였다. Zaho *et al.*(2014)은 화이트 햇 커뮤니티의 웹 취약점 공개에 영향을 미치는 요인을 분석하였다. 더 많은 참여(화이트 해커의 유명세, 취약점 수 및 심각도, 목적 웹사이트 유형)와, 행동(제출된 보고서 수, 취약점 유형, 취약점 발견 전략)이 화이트 해커의 취약점 발견 프로세스에 생산성을 더 높인다는 결과를 도출하였다. Algarni *et al.*(2014)은 취약점 발견자와 수요자의 상호행동의 역할에 대한 연구가 부족한 상황에서, 실제 취약점마켓을 대상으로 보고서와 설문지를 토대로 취약점마켓 메커니즘(생산자 → 취약점마켓 → 고객 → 공격/해결)을 분석하였다. 연구결과, 취약점마켓 참여자들이 습관 및 일상 선택, 호기심, 재미, 이익, 감사, 새로운 발견 기술 배우기, 열정과 같은 이유로 취약점마켓에 참여하는 것을 발견하였다. 특히 많은 취약점 발견자들이 보안 회사에서 성공적인 커리어를 마치고 은퇴한 후, 취약점마켓에 참여하는 것을 확인하였다.

2.2 보안 연구자

2.2.1 보안 연구자 정의 및 분류

본 연구에서는 보안 연구자(Security Researcher)와 유사한 특징을 갖고 있는 해커에 대한 선행연구를 고찰하였다. 해커(Hacker)는 일반인이 알고 있는 범죄자가 아닌 컴퓨터 프로그래밍 기술을 가진 개인을 의미한다(Chan and Yao, 2011). 법을 위반하는 해커를 나타내는 용어는 범죄적 해커(Criminal Hacker) 또는 크래커(Cracker)로 정의된다(Fitch, 2004). 본 연구에서는 해커에 대한 다양한 정의를 <표 1>, <표 2>로 정리하였다(Fitch, 2004; Kesan and Hayes, 2016). 에이쓰리시큐리티(2010)에 따르면 초창기 해커들이 컴퓨터의 취약점을 조작하여 의도된 동작을 수행토록 하는 익스플로잇(Exploit) 동기는 순수한 연구, 자기만족과 같은 것이었지만 현재 해커는 익스플로잇 동기는 금전적 이익을 얻기 위한 경향이 강하다. 미공개 취약점을 거래하던 과거와 달리 현재에는 취약점 거래(Exploit Trade) 행위에 대한 사람들의 시각이 달라짐을 알 수 있다.

〈표 1〉 목적에 따른 해커분류

구 분	설명
Whitehat	- 해커 윤리법을 준수하며 보안 전문가로서 일함 - 대부분의 해커들은 화이트 해커를 컴퓨터 시스템 보안을 향상시키고 시스템, 소프트웨어, 네트워크를 운영하는데 흥미가 있음
Blackhat	- 블랙햇의 동기는 힘과 권력이고 자신들의 행동을 합리화하고 해킹행위 지속 수행함 - 분노, 증오, 웹 파괴 - 침투한 네트워크의 데이터를 훔치거나 파괴하는데 거리낌 없음
Grayhat	- 잘 알려진 올드 스쿨 해킹 그룹 중 하나인 L0pht에 의해 만들어짐 - 기업의 보안 테스터 및 악의적인 블랙햇과 거리를 둠 - 다수의 기업 보안 연구자, 보안 전문가 및 컨설턴트를 포함

〈표 2〉 윤리와 도덕적 기준으로 구분한 해커분류

구 분	합법적인	중립적인	혼돈, 무차별
선의	벤더의 제품 안에 있는 취약점을 찾기 위해 벤더에게 고용된 해커	공공재에 대한 취약점 발견을 위한 인가되지 않은 테스팅	핵티비즘
중립	방어 시설을 향상시키기 위해 취약점 지식을 사용하는 정부	호기심으로 동기가 부여된 해킹 행위	재미를 위한 해킹(lulz)
악의	반대자를 제압하기 위해 법적으로 허용된 스파이웨어를 사용하는 정부	디지털 사기 및 절도를 위한 해킹	위해를 가하기 위한 해킹(DDoS (Distributed Denial of Service, 데이터 절도, 랜섬웨어)

이상의 논의를 통하여 보안 취약점 정보를 찾을 수 있는 능력을 가진 보안 연구자의 역할이 중요해질 것으로 예상된다.

2.2.2 해커의 동기 연구

본 연구에서는 실증적 연구기법으로 해커의 해킹의도를 연구한 논문을 중심으로 해커의 행동에 영향을 미치는 것이 무엇인지 살펴보았다(Beebe and Guynes, 2006; Chan *et al*., 2005; Giboney *et al*., 2016; Owen, 2016; Young *et al*., 2007). Chan *et al*.(2005)은 중독, 내재적 동기, 자기점검 이론으로 해킹 행위를 확인하기 위하여 62명의 해커를 대상으로 연구한 결과, 첫째, 흥미와 즐거움의 목적으로 해커 활동을 하는 개인은 발각될 가능성과 규제기관에 부과되는 규칙에 덜 좌절하고 둘째, 해킹하는데 높은 동기를 가진 사람은 발각될 가능성, 종사자들에 의해 부과된 규칙 그리고 규제 기관에 의해 부과된 규칙과 같은 세 가지 억제요인에 덜 좌절하고 셋째, 높은 자기점검 경향이 있는 자와 비교해서 낮은 자기점검 경향이 있는 자는 억제요인에 더 좌절하고 마지막으로 가치, 신념, 자아상과 같은 내부적 요인이 억제요인에 덜 좌절하는 요인인 것을 발견했다. Beebe and Guynes(2006)은 해커의 행동 예측 모델을 연구하기 위하여 규모가 큰 해커 행사인 DefCon과 BlackHat 컨퍼런스의 참가자와 학생 546명을 대상으로 설문을 실시하였다. 독립변수로 성별, 나이, 교육 수준, 전문화 상태, 개인의 도덕적 철학(이상주의, 상대주의), 종속변수로 해커 행동 그리고 조절변수로 해킹에 대한 윤리적 태도와 신념으로 설정하여 측정하였다. 연구결과, 젊은 사람이 나이든 사람보다, 일반 컴퓨터 사용자가 컴퓨터 전문가보다 불법적 해킹에 대한 관점이 더 우호적이다. 그리고 불법적 해킹에 대한 태도는 해킹에 대한 누군가의 의지에 영향을 미치는 것으로 나타났다. 이 연구의 특이점은 해킹 의도를 측정하여 'blackhat', 'ex-blackhat', 'whitehat', 'nohat'으로 해커의 유형을 분류하는 척도를 제시한 것이다. Young *et al*.(2007)은 해커의 생각을 연구하기 위하여 매년 라스베가스에서 열리는 해커 행사인 DefCon 컨퍼런스에 참가한 해커 54명, 컨퍼런스 참여자 73명을 대상으로 해커의 심리를 측정하고 분석하였다. 해커가 엄격한 사법적 처벌을 인지함에도 불구하고 불법적 해킹 행위를 계속하는 것과 해커가 해킹 행위로부터 높은 효용가치, 적은 비공식적 제재, 검거와 처벌에 대한 낮은 가능성을 인지하는 것을 밝혀냈다. Owen(2016)은 합리적 선택이론(Theory of Reasoned Action, TRA)과 일반억제이론(General Deterrence Theory, GDT)의 관점에서 해커의 동기와 의욕상실에 영향을 미치는 요인을 측정하기 위하여 Delta Hack 컨퍼런스에 참가한 107명의 해커를 대상으로 연구를 진행하였다. 숙달, 호기심과 같은 개인적 요소와 복잡성과 같은 업무적 요소가 해커의 태도에 영향을 미치고 해커의 태도, 주관적 규범, 처벌의 확실성이 해킹의도에 영향을 미치는 것을 밝혀냈다. Giboney *et al*.(2016)은 기존 연구자들이 해커들이 갖고 있는 지식과 기술에 대한 검증 능력의 부족에 대한 문제의식을 갖고 해커의 전문지식 측정 도구 개발을 위하여

보안 전문지식 평가 모델을 제안하였다. 보안 전문가는 해당 분야의 원리를 기반으로 문제를 조직하기 위해 추상적 분류에 의존하고, 신입 전문가는 물리적 증거, 명쾌한 언어 그리고 공식화를 기반으로 문제를 조직한다.

2.3 연구변수

2.3.1 취약점 연구 자기효능감

현대 심리학에서는 인간의 행동을 보다 체계적으로 이해하기 위해서 인간의 행동 변화와 영향을 설명하기 위한 주요 변수로 자기효능감을 주목하고 있다. 자기효능감(Self-Efficacy)이란 '특정한 행동을 실행하기 위한 기술과 능력을 조직화하거나 수행하는 것에 대한 자신의 판단'이다(Bandura, 1982). 새로운 기술 및 서비스가 등장할 때마다 자기효능감 변수를 통해서 사람의 행동을 예측하기 위한 다양한 연구가 진행되고 있다(Bandura, 1991; Compeau and Higgins, 1995; Giboney *et al*., 2016; Lent *et al*., 1984; Locke and Latharm, 1990; 박상호, 2011). Locke and Latharm(1990)에 따르면 자기효능감이 강할수록 사람들은 스스로 높은 목적에 도전하고 목적을 실행하는데 더욱 전념하며 분석적 사고를 사용한다고 하였다. 즉, 특정 부분에서 자기효능감이 낮은 사람들은 어려운 과제를 위협으로 인식하고 기피하지만 자기효능감이 높은 사람들은 어려운 과제를 헤쳐 나가야 할 도전으로 본다. 또한 직무를 수행함에 있어서 자기효능감은 개인의 행동에도 영향을 미치는데, Lent *et al*.(1984)의 연구에 따르면 과학적 지식을 익힐 때 자기효능감을 인지하는 사람이 성공적인 학습과정과 인내심을 얻게 된다고 주장하였다. Bandura(1991)는 결과에 대한 기대와 가치만으로는 높은 난이도의 작업을 수행하기 위한 동기를 유발하기에는 충분하지 못하다고 주장하였다. Compeau and Higgins(1995)는 컴퓨터 자기효능감(Computer Self-Efficacy, CSE)을 '컴퓨터를 사용하는 능력에 대한 개인적인 판단'으로 정의하였다. 이러한 컴퓨터 자기효능감 변수는 디스켓 포맷이나 스프레트시트 수식과 같은 간단한 작업보다는 오히려 컴퓨터를 통한 서면 보고서 작성 또는 재무 데이터 분석에 대한 자기효능감을 측정하는 도구로 사용되었다. 박상호(2011)는 인터넷 자기효능감이 인터넷 몰입에 긍정적인 영향을 미치는 것을 발견하였다. 최근에는 해커의 전문지식을 측정하기 위한 시도로서 컴퓨터 자기효능감 변수가 사용되고 있다. Giboney *et al*.(2016)은 초보해커와 전문가해커의 전문지식을 측정하기 위하여 컴퓨터 자기 효능감이란 개념을 사용하는 시도를 하였다. 이상의 논의를 통해 본 연구에서는 보안 연구자의 취약점 연구 자기효능감이 보안 연구자의 취약점 연구 동기를 설명하는 주요 요인으로 보았다.

2.3.2 몰입

내적동기를 설명하는데 가장 수준 높은 이론은 긍정심리학자 Csikszentmihalyi가 제안한 몰입이론(Flow Theory, FT)이다. Csikszentmihalyi(1975)는 몰입(Flow)이란 '어떠한 활동에 깊게 몰두하여 이전 행동을 자연스럽게 따르며 그 과정이 무의식 상태'라고 정의하였다. 또한 Csikszentmihalyi는 몰입경험에 대한 전제는 누군가의 기술과 과제에 대한 도전의 정확한 매칭(Matching)이라고 하였다. 몰입을 경험하기 위해서는 경험하기 위한 기술과 도전의 수준은 낮지 않아야 한다. 만약, 사람들이 배우고자 하는 기술 및 수준이 낮으면 결국 무관심에 이르게 된다. 즉, 몰입경험은 개인의 기술 최첨단(Cutting Edge)에 놓여 있으며 유동적인 목표가 된다. 따라서 사람들은 새로운 기술이 생기면 이러한 기술을 습득하기 위해 많은 도전을 시도하게 되고 이러한 선택은 기술의 갱신으로 이어진다. 수십 년 동안 몰입에 대한 연구를 진행하면서 Csikszentmihalyi(2006)는 사람들은 몰입을 경험할 때 목표의 분명함, 즉각적인 피드백, 기회와 능력 사이의 균형유지, 집중력 강화, 현재 일을 중요시함, 쉬운 통제, 시간 왜곡, 자아 상실을 경험한다고 하였다.

몰입 개념은 IT 전문가 및 e-Shopper 등의 분야에서 일하는 사람들의 동기를 설명하고 해석하는데 유용하게 사용된다(Ha, 2007; Hoffman *et al*., 2003; Hsu and Lu, 2004). Hoffman *et al*.(2003)은 경험이 풍부한 사용자는 그렇지 않은 사용자와 비교하여 더 높은 수준의 몰입을 경험하는 것을 발견하였다. Hsu and Lu(2004)는 신뢰와 몰입 이론을 통합하여 모바일 뱅킹 사용자의 수용에 대한 연구를 진행하였다. 연구결과, 모바일 뱅킹 사용자의 몰입 경험이 모바일 뱅킹 사용 의도를 예측하는 요인으로 확인되었다. Ha(2007)의 연구에서는 몰입 경험이 온라인 게임의 수용에 영향을 미치는 요인인 것을 발견하였다.

해커 연구 분야에서도 몰입은 해커의 해킹 동기를 설명하기 위한 측정도구로 사용되고 있으며 이에 대한 주요 연구는 다음과 같다(Beveren, 2001; Voiskounsky and Smyslova, 2003; 박찬현 등, 2016; 우형진, 2004). Beveren(2001)가 주장한 해커는 몰입을 경험할 수 있다는 가정 하에 Voiskounsky and Smyslova(2003)은 몰입, 컴퓨터 사용기간, 알려진 SW제품 다양성 요인을 측정도구로 삼아 해커를 대상으로 군집분석(Cluster Analysis)을 실시하였다. 연구결과, 몰입이 컴퓨터 해커의 행동에 영향을 미치는 요인이라는 것을 경험적 연구로 입증하였다. 국내의 연구자들도 몰입이란 개념을 해커의 행동을 설명하는 개념으로 사용하고 있다. 우형진(2004)은 심리학 분야에서 최적경험개념과 공포관리이론(Terror Management Theory, TMT)을 토대로 해커를 대상으로 요인분석을 실시하였다. 연구결과, 해킹을 하면서 높은 몰입을 인지하는 해커들이 해킹빈도와 해킹유형과 같은 해킹경험이 많이 있음을 발견하였다. 박찬현 등(2016)은 회귀분석을 통하여 해커의 탈선적 해킹행동을 설명하려는 연구를 진행하였으며 몰입이 탈선적 해킹경험에 영향을 미치는 주요 변수라는 것을 발견하였다. 따라서 해커는 창의적이고 순수한 연구동기와 목적으로 새로운 보안 취약점 및 익스플로잇을 발견하는 동안에 몰입을 경험할 가능성이 높다. 이상의 논의를 토대로 본 연구에서는 몰입을 보안 연구자가 취약점을 연구하면서 인식하게 되는 요인으로 보았다.

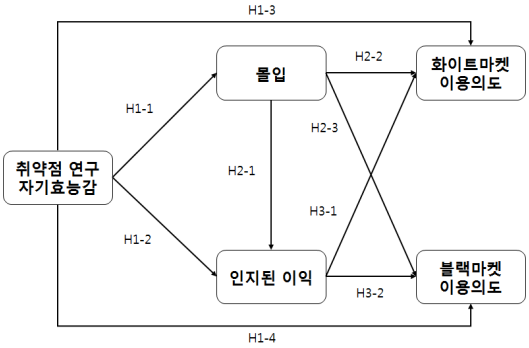
2.3.3 취약점마켓 이용의도

취약점마켓은 편의상 합법과 비합법으로 구분하여 화이트마켓, 블랙마켓, 그레이마켓으로 구분된다. 취약점 정보활용에 관한 이슈는 다음과 같다. Algarni *et al*.(2014)의 연구에 따르면 취약점마켓에서 발견자 대다수는 소프트웨어 벤더와 제휴하기보다는 발견한 취약점을 자유롭게 퍼뜨렸고 그 결과로 취약점마켓에 대한 합법(White), 비합법(Black)의 이슈가 발생한다고 하였다. Egelman *et al*.(2013)에 따르면 정보보안 관련 학계에서도 취약점 정보의 활용에 대한 윤리적 이슈에 대한 논의가 이루어지고 있다고 하였다. 본 연구에서는 취약점마켓 이용의도를 측정하기 위하여 선행연구를 토대로 화이트마켓, 블랙마켓에서 각각 구분되는 특성으로 가격, 취약점 활용 예상, 합법유무로 설문문항을 제작하였다(<표 6> 참조). 본 연구는 연구모형의 경로를 명확하게 파악하기 위하여 화이트마켓과 블랙마켓의 중간에 있는 그레이마켓 이용의도에 대한 측정은 배제하였다.

Ⅲ. 연구모형 및 가설설정

3.1 연구모형

본 연구의 목적은 '보안 연구자들의 취약점 연구동기가 무엇인가? 이러한 요인들이 취약점마켓 이용의도에 어떠한 영향을 미치는가?'에 대한 질문으로부터 시작되었다. 본 연구의 연구모형은 취약점마켓, 취약점마켓 참여자, 해커에 대한 논문 및 보고서 등과 같은 선행연구 분석을 통해 취약점 연구동기(취약점 연구 자기효능감, 몰입, 인지된 이익)와 취약점마켓 이용의도(화이트마켓 이용의도, 블랙마켓 이용의도) 변수를 도출하였다. 본 연구의 연구모형은 <그림 2>와 같다.



〈그림 2〉 본 연구의 연구모형

3.2 연구가설

3.2.1 취약점 연구 자기효능감 가설

Bandura(1982)는 자기효능감을 '특정한 행동을 실행하기 위한 기술과 능력을 조직화하거나 수행하는 것에 대한 자신의 판단'으로 정의하였다. 그리고 이 개념이 자신이 가진 실제 능력을 판단하는 것이 아니라 자신의 능력에 대한 개인적인 판단이라고 설명하였다. 이러한 자기효능감은 사람의 동기부여에 대한 효과를 설명하는 주요 변수로 작용한다. 자기효능감 변수를 통해서 사람의 행동을 예측하기 위한 연구가 진행되고 있다. 본 연구에서는 이러한 자기효능감 개념을 취약점 연구로 확장하여 취약점 연구 자기효능감(Vulnerability Research Self-Efficacy, VRSF)이라는 개념을 도출하였다.

본 연구에서는 보안 연구자가 취약점 연구에 대한 자기효능감이 높을수록 취약점 연구를 통한 몰입경험에 대해 유의한 영향을 미칠 것으로 보았다. 이러한 자기효능감과 몰입에 대한 선행연구는 다음과 같다. 박상호(2011)는 인터넷 자기효능감이 인터넷 몰입에 긍정적인 영향을 미치는 것을 확인하였다. 배현숙(2015)의 연구에서는 항공사 객실승무원 중에서 자기효능감이 높은 집단은 조직몰입을 높이는데 유의한 영향을 미치는 것을 확인하였다. 김기병 등(2015)은 자기효능감의 측정항목 중에서 일에 대한 자신감, 자기조절 효능감이 관광 몰입에 유의한 영향을 미치는 것을 확인하였다.

취약점 연구에 대한 자기효능감이 높은 보안 연구자는 취약점 연구를 통해 이익을 인지할 것으로 보았다. 김용일, 양현교(2012)의 연구에서는 컴퓨터 자기효능감이 POS 정보시스템에 대한 업무성과에 유의한 영향을 미친다는 것을 확인하였으며, 성행남(2014)은 모바일 학습에 대한 자기효능감이 성과기대에 유의한 영향을 미친다는 것을 발견하였다. 또한 Giboney *et al.*(2016)의 연구에는 해커의 컴퓨터 자기효능감이 해킹전문지식의 학습(또는 획득)에 유의한 영향을 미치는 것을 확인하였다.

취약점 연구에 대한 자기효능감을 갖는 보안 연구자는 취약점마켓 이용의도가 있을 것이다. 자기효능감이 정보기술의 이용의도 미치는 영향에 대해 다수의 연구가 있다. Chau(2001)의 기술수용모형(Technology Acceptance Model, TAM)을 활용한 정보기술 이용의도에 대한 연구에서는 자기효능감이 이용의도에 유의한 영향을 미치는 것을 확인하였다. Venkatesh *et al.*(2003)은 이용의도를 '주어진 기술에 대해 사용자의 실제 이용에 직접적으로 영향을 미치는 정도'라고 정의하였다. 본 연구에 선행연구를 토대로 취약점마켓 이용의도(Vulnerability Market Use Intention, VMUI)를 '보안 연구자가 취약점마켓이 생길 경우 이용하는 정도'로 정의하였고 세부적 항목을 취약점마켓 선행연구에서 제시된 취약점마켓의 이용의도 요인을 가격, 취약점 정보활용, 법제화 유무로 구분하였다(Ablon *et al.*, 2014; Algarni *et al.*, 2014; Egelman *et al.*, 2013). 그 결과 본 연구에서는 화이트마켓 조건(블랙마켓 보다 비싼 취약점 정보 가격, 취약점 정보가 소프트웨어 문제 해결기대, 취약점마켓 법제도가 생길 경우 화이트마켓 이용의도), 블랙마켓 조건(화이트마켓 보다 비싼 취약점 정보 가격, 취약점 정보 악용 예상, 취약점마켓 법제도가 없을 시 블랙마켓 이용)으로 제시하여 설문 측정도구를 제작하였다.

이상의 논의를 통하여 본 연구에서는 취약점 연구 자기효능감을 '보안 연구자가 취약점 분석 도구를 활용하여 연구를 수행하는 경우 자신의 능력을 지각하는 개인적인 판단'이라고 정의하였다. 본 연구의 취약점 연구 자기효능감 측정도구는 Giboney *et al.*(2016)이 해커들을 대상으로 측정한 컴퓨터 자기효능감 측정도구 10가지 중 유의하다고 판단된 '시간 투자', '방법 도움', '사전 취약점 도구 이용 경험', '타인의 도움', '위급 시 도움 요청' 요인을 본 연구의 목적에 맞게 수정하여 사용하였다. 따라서 본 연구에서는 보안 연구자가 취약점 연구에 대한 자기효능감이 높을수록 취약점 연구를 통해 몰입, 인지된 이익, 취약점마켓 이용의도에 유의한 영향을 미칠 것으로 보았다. 이상의 논의를 본 연구에 적용하여 다음과 같은 가설을 도출하였다.

H1-1: 보안연구자의 취약점 연구 자기효능감은 몰입에 유의한 영향을 미칠 것이다.
H1-2: 보안연구자의 취약점 연구 자기효능감은 인지된 이익에 유의한 영향을 미칠 것이다.
H1-3: 보안연구자의 취약점 연구 자기효능감은 화이트마켓 이용의도에 유의한 영향을 미칠 것이다.
H1-4: 보안연구자의 취약점 연구 자기효능감은 블랙마켓 이용의도에 유의한 영향을 미칠 것이다.

3.2.2 몰입 가설

Csikszentmihalyi(1975)는 몰입을 '어떠한 활동에 깊게 몰두하여 이전 행동을 자연스럽게 따르며 그 과정이 무의식 상태'라고 정의하였다. 몰입은 IT 전문가, e-Shopper, 게임, 컴퓨터 응용 등 많은 분야에서 사용되고 있다(Ha, 2007; Hoffman *et al.*, 2003; Hsu and Lu, 2004). 최근 국내에서 진행된 몰입 관련 연구를 살펴보면 다음과 같다. 이현지, 정동훈(2012)은 몰입 경험이 스마트폰 게임센서 이용의도에 유의한 영향을 미치는 것으로 나타났다. 박신영(2013)은 사람들이 스마트폰을 이용함에 있어 몰입을 경험하면 긍정적 감정, 충족감과 같은 정서를 매개로 스마트폰 이용의도에 유의한 영향을 미치는 것을 확인하였다. 또한 허지현(2013)은 몰입 경험이 온라인 여행커뮤니티 이용의도에 영향을 미치는 것을 확인하였다. 그리고 진경미와 장순자(2016)의 연구에서도 항공사 모바일 앱 이용자의 몰입 경험이 항공사 모바일 앱 이용의도에 유의한 영향을 미치는 것으로 나타났다.

보안 연구자와 유사한 특성을 갖는 집단인 해커의 해킹동기를 설명하는 변수에도 몰입 경험에 대한 연구가 진행되었다. Voiskounsky and Smyslova (2003)의 연구에서는 몰입 경험이 컴퓨터 해커의 행동에 유의한 영향을 미치는 요인인 것을 확인하였다. 또한 우형진(2004)의 연구에서도 높은 몰입을 인지하는 해커들이 해킹경험이 많이 있는 것을 확인하였다. 그리고 박찬현 등(2016)의 연구에서도 몰입 경험이 탈선적 해킹경험에 유의한 영향을 미치는 주요 변수인 것을 확인하였다. 따라서 몰입 또한 보안 연구자의 연구동기로 고려될 수 있는 주요 요인 중 하나라고 보았다. 이렇게 몰입 경험을 하는 보안 연구자는 <표 6>에서 설명된 바와 같이 취약점마켓 참여 동기로 주로 금전적 이익이나 주관적 의미부여와 같은 본 연구에서 정의한 인지된 이익을 느끼는 것으로 보았다. 이상의 논의를 통하여 본 연구에서는 몰입을 '보안 연구자가 취약점 연구에 몰두하게 되면서 다른 것들을 의식하지 못하는 상태'라고 정의하였다. 이상의 논의를 통하여 본 연구에서는 보안 연구자의 취약점 연구에 대한 몰입 경험은 인지된 이익, 취약점마켓 이용의도에 유의한 영향을 미칠 것으로 보았으며 이를 본 연구에 적용하여 다음과 같은 가설을 도출하였다.

H2-1: 보안연구자의 몰입은 인지된 이익에 유의한 영향을 미칠 것이다.
H2-2: 보안연구자의 몰입은 화이트마켓 이용

의도에 유의한 영향을 미칠 것이다.

H2-3: 보안연구자의 몰입은 블랙마켓 이용의도에 유의한 영향을 미칠 것이다.

3.2.3 인지된 이익 가설

본 연구에서는 취약점마켓 이용자 및 해커에 대한 선행연구를 토대로 인지된 이익 요인을 도출하였고, 보안 연구자가 취약점 연구를 통해 기대하는 요인을 다섯 가지로 구분하였고 관련된 연구는 다음과 같다. 첫째, 보안 연구자는 금전적 이익을 기대한다. Algarni *et al.*(2013)의 연구에서는 성공적인 취약점 발견자는 금전적 보상에 상당한 동기를 갖고 있음을 발견하였다. 또한 Finifter *et al.*(2013)의 연구에 따르면 기발한 취약점을 발견할 수 있는 보안 전문가들은 이에 상응하는 보상금을 받길 원한다고 하였다. Zaho *et al.*(2014)에 따르면 화이트 해커가 자신의 유명세를 높이려는 목적으로 취약점을 발견하는데 더욱 열중하는 것을 확인하였다. 해커는 종종 실력과시 및 명성을 높이려는 목적으로 취약점 패치 전에 해당 소프트웨어를 공격하여 금전적 이익을 취하려는 제로데이 공격을 시도하기도 한다. 이러한 아이디어에 착안해서 버그 바운티 서비스를 제공하는 Bugcrowd와 Cobalt에서도 취약점 발견 정도에 따라 보안 연구자들을 명예의 전당(Hall of Fame)에 이름을 올리는 서비스를 제공하고 있다. 셋째, 보안 연구자는 해킹기술 역량향상을 기대한다. Giboney *et al.*(2016)에 따르면 전문적인 기술을 가진 해커들은 해당 시스템의 도메인의 원리를 기반으로 문제를 조직화하여 추상적인 분류로 이해한다고 하였다. 반면에 초보적인 해커들은 물리적 증거, 명백한 단어, 공식에 의존하여 문제를 해결하는 습성을 보인다고 하였다. Algarni *et al.*(2014)의 연구에 따르면 보안 연구자는 취약점마켓 참여를 통해 새로운 취약점 발견 기술을 배우는 것을 확인하였다. 마지막으로, 보안 연구자는 지적호기심 충족 및 주관적의미를 기대한다. Owen(2016)의 연구에 따르면 호기심은 해커를 상황 변화에 대한 지식을 살피기 위한 새로운 접근법을 시도하는 길로 이끈다고 하였다. 이에 본 연구에서는 인지된 이익을 '보안 연구자가 보안 취약점을 연구하거나 찾는 행위로 얻게 되는 기대 편익'이라고 정의하였다.

실제 취약점마켓을 운영함에 있어서 취약점마켓 운영주체가 보안 연구자에 대해 본 연구에서 제시한 인지된 이익을 고려하는 것을 알 수 있다. 예를 들면, 기업을 대상으로 버그 바운티 서비스를 제공하는 버그크라우드(2015)는 보안 연구자들이 취약점마켓에 참여하는 동기를 금전적 수익, 명성, 기술 유지, 취미, 도전 등으로 선정하였다. 이를 본 연구에 적용하여 인지된 이익을 측정하는 항목으로 활용하였다. 본 연구에서는 보안 연구자가 취약점 연구를 통해 취약점 정보의 가치에 대한 인지된 이익이 취약점마켓 이용의도에 유의한 영향을 미칠 것으로 보았다. 이상의 논의를 본 연구에 적용하여 다음과 같은 가설을 도출하였다.

H3-1: 보안연구자의 인지된 이익은 화이트마켓 이용의도에 유의한 영향을 미칠 것이다.

H3-2: 보안연구자의 인지된 이익은 블랙마켓 이용의도에 유의한 영향을 미칠 것이다.

Ⅳ. 연구방법

4.1 설문조사

본 연구의 분석단위는 개인이며 시스템, 네트워크, 웹 애플리케이션 취약점을 진단할 수 있는 기술적 능력을 갖고 있거나 학습하는 사람을 대상으로 설문지 방법에 의한 조사를 실시하였다. 본 연구에서는 표본의 대표성을 확보하기 위하여 보안 취약점 정보를 접하기 쉬운 환경에 있는 보안 취약점 분석 및 모의해킹 업무 경험을 가진 보안 연구자를 본 연구의 연구대상으로 설정하였다. 본 연구는 일반인이 아닌 보안 취약점 연구 경험 및 모의해킹 업무 경험이 있는 표본을 대상으로 설문조사를 실시하였다.

설문지 배포에 앞서 정보보안 전문가들을 대상으로 인터뷰(Interview) 및 파일럿 테스트(Pilot Test)를 실시함으로써 설문방법 및 측정항목들의 타당성을 검토하였다. 검토를 마친 후 본 설문에 대한 표본의 대표성을 확보하기 위해 설문지 앞부분에 취약점 진단 및 해킹 기술 경험 등에 관한 항목을 추가하였다. 이와 동시에 표본의 타당성 및 신뢰도를 높이기 위하여 설문지 초반부에 보안 취약점 연구 경험, 해킹 경험, 보안 관련 자격증 유무 그리고 취약점 종류에 대한 기초적인 지식 유무를 측정도구로 제작하였고 설문지 후반부에는 설문대상자의 '개인정보 수집 및 이용 동의'와 '이메일 주소' 수집을 통해서 표본의 중복가능성을 최소화 하도록 제작하였다. 설문지 제작 후 설문지 테스트 결과 보안 용어를 모르거나 보안 취약점 정보 가치를 인식하지 못하는 사람의 대다수는 제대로 설문에 응하지 못하거나 도중에 포기하는 반응을 보였다. 따라서 본 연구의 설문지는 적절하게 작성되었다고 판단할 수 있다.

본 연구는 2016년 11월 1일부터 11월 15일까지 총 2주 동안 설문지 수집을 실시하였다. 우선 구글독스(Google Docs)를 활용하여 온라인 설문지를 작성하였고, 정보보안 전문 카페, 정보보안 관련 페이스북(Facebook) 페이지 등에 설문지 관련 링크를 게시하여 설문 희망자에 한하여 설문지를 배포하였다. 또한 정보보안 관련 오프라인 세미나에 참여하여 설문지를 배포 하였다. 설문지 배포 결과, 취약점 분석경험에 체크한 총 215부의 설문지를 회수하였고, '취약점 분석경험 없음'에 표시하거나 응답이 불성실하다고 판단된 설문지 총 61부를 제거하여 최종 유효 설문지 154부를 본 연구에서 제시한 모형을 검증하기 위해 사용하였다.

연구모형 검증 전 적절한 표본의 수를 확보하는 작업은 중요하며 이에 대하여 학자들 마다 다양한 견해를 제시하였다(우종필, 2014). 본 연구에서는 표본의 수에 대한 기준을 Mitchell(2001)의 변수 당 10~20배, Stevens(2012)의 변수 당 15배가 필요하다는 주장을 인용하였다. 본 연구의 표본은 154부, 관측변수는 5개이므로, Mitchell(2001)과 Stevens(2012)가 주장한 표본의 수 기준을 충족하였다.

회수된 설문 데이터를 통계분석 프로그램 SPSS 21을 이용하여 빈도분석을 실시하였다. <표 3>에는 보안 취약점 연구 경험자들의 기본적인 인구통계학적 및 취약점 연구 경험에 대한 정보가 정리되어 있다. 본 연구의 응답자 성별은 남성이 134명(87%)으로, 여성 20명(13%)보다 많았다. 연령대는 15세 이상~20세 미만이 12명(7.8%), 20세 이상~25세 미만이 32명(20.8%), 25세 이상~30세 미만이 64명(41.6%), 30세 이상~35세 미만이 24명(15.6%), 35세 이상~40세 미만이 6명(3.9%), 40세 이상이 16명(10.4%)으로 실무에서 정보보안 업무를 수행할 것으로 추정되는 25세 이상 응답자 비율이 70%를 넘는다. 최종학력은 고등학교 졸업 32명(20.8%), 대학교 졸업 88명(57.1%), 석사 졸업 26명(16.9%), 박사 졸업 6명(3.9%), 기타 2명(1.3%)으로 응답자의 약 80%가 대학교 졸업 이상의 고학력자 집단에 속한다.

본 연구의 응답자 중 취약점 분석경험은 154명(100%), 모의해킹 업무경험은 96명(62.3%), 대학 정보보호 연합동아리(Korea University Clubs Information Security, KUCIS) 참여경험은 40명(26%), 버그 바운티(Bug Bounty Program, BBP) 대회 참여경험은 32명(20.8%), 차세대 보안리더 양성 프로그램(Best of The Best, BoB) 참여경험은 12명(7.8%)으로 나타났다. 응답자 절반 이상이 취약점 분석경험을 가졌으며 모의해킹 업무경험이 있는 것으로 나타났다. 반면 KUCIS, 버그 바운티, BoB 참여 비율이 저조한 것을 알 수 있다.

본 연구에서는 응답자의 정보보호 관련 자격증 보유 여부를 확인하기 위하여 국제 자격증(CISSP, CISA, CEH, CISM, CHFI), 국내 자격증(정보보안기사, 정보보안산업기사, CPPG, 디지털 포렌식 전문가 2급)으로 각각 구분하여 질문하였다. 응답자의 자격증 보유 현황은 정보보안기사 36명(23.4%), CISSP(Certified Information System Security Professional) 20명(13%), CEH(Certified Ethical Hacker)

〈표 3〉 표본의 인구통계학적 특성

구 분		응답자 수	비율
성별	남성	134명	87%
	여성	20명	13%
연령	15세 이상 ~ 20세 미만	12명	7.8%
	20세 이상 ~ 25세 미만	32명	20.8%
	25세 이상 ~ 30세 미만	64명	41.6%
	30세 이상 ~ 35세 미만	24명	15.6%
	35세 이상 ~ 40세 미만	6명	3.9%
	40세 이상	16명	10.4%
최종학력	고등학교 졸업	32명	20.8%
	대학교 졸업	88명	57.1%
	석사 졸업	26명	16.9%
	박사 졸업	6명	3.9%
	기타	2명	1.3%
취약점 분석경험	예	154명	100%
모의해킹 업무경험	예	96명	62.3%
	아니오	58명	37.7%
버그 바운티 참여경험	예	32명	20.8%
	아니오	122명	79.2%
BoB 참여경험	예	12명	7.8%
	아니오	142명	92.2%
KUCIS 참여경험	예	40명	26%
	아니오	114명	74%
합계		154명	100%

18명(11.7%), CISA(Certified Information Systems Auditor) 18명(11.7), CPPG(Certified Privacy Protection General) 14명(9.1%), 정보보안 산업기사 16명(10.4%), 디지털 포렌식 전문가 2급 6명(3.9%), CHFI(Computer Hacking Forensic Investigator) 4명(2.6%), CISM(Certified Information Security Manager) 4명(2.6%), 기타(리눅스마스터 2급, 정보처리기사, SW 보안약점진단원, EnCE 등) 8명(5.2%) 순으로 나타났다(<표 4> 참조). 이를 통하여 보안 연구자들은 기대한 것보다 적은 수의 정보보호 관련 자격증을 취득한 것을 알 수 있다.

응답자들의 해킹기술 습득경로와 실습환경을 분류하면 <표 5>와 같다. 먼저 응답자의 해킹기술 습득경로는 커뮤니티 활동 94명(61%), 교육기관 88명(57.1%), 컨퍼런스 60명(39%), 해킹대회 48명(31.2%), SNS 42명(27.3%), 기타(주로 독학, 업무 등) 22명(14%) 순으로 나타났다. 그리고 응답자의 해킹기술 실습환경은 가상환경 124명(80.5%), 허가된 시스템 90명(58.4%), 워게임(War Game) 74명(48.1%), 해킹대회 52명(33.8%), 기타 2명(1.3%) 순으로 나타났다. 이를 통하여 응답자의 절반 이상이 보안 전문 카페나 소모임 같은 커뮤니티 활동과 정보보호 전문 교육기관을 통하여 해킹기술을 습득하는 것으로 나타났다. 또한 습득한 해킹기술을 구현하기 위하여 응답자 절반 이상이 가상환경을 구축하거나 허가된 시스템을 이용하므로 비교적 안전하고 합법적인 공간에서 해킹기술을 실습하는 것을 알 수 있다.

〈표 4〉 표본의 자격증 보유 현황

구 분		응답자 수	비율
국제 자격증	CISSP	20명	13%
	CISA	18명	11.7%
	CEH	18명	11.7%
	CISM	4명	2.6%
	CHFI	4명	2.6%
국내 자격증	정보보안기사	36명	23.4%
	정보보안산업기사	16명	10.4%
	CPPG	14명	9.1%
	디지털 포렌식 전문가 2급	6명	3.9%
기타		8명	5.2%

〈표 5〉 표본의 해킹기술 습득경로 및 해킹기술 실습환경

구 분		응답자 수	비율
해킹기술 습득경로	커뮤니티 활동	94명	61%
	SNS	42명	27.3%
	해킹대회	48명	31.2%
	컨퍼런스	60명	39%
	교육기관	88명	57.1%
	기타	22명	14.3%
해킹기술 실습환경	허가된 시스템	90명	58.4%
	가상환경	124명	80.5%
	해킹대회	52명	33.8%
	워게임	74명	48.1%
	기타	2명	1.3%

4.2 측정도구 개발

본 연구에서는 취약점마켓 이용자에 대한 연구와 해커에 관한 연구를 토대로 보안 연구자의 취약점 연구 행동에 미치는 주요 변수를 도출하였다. 도출된 취약점 연구 자기효능감, 몰입, 인지된 이익, 화이트마켓 이용의도, 블랙마켓 이용의도에 대한 선행연구를 검토한 후 본 연구에 맞게 수정하였다(<표 6> 참조). 연구목적에 맞게 수정된 설문지의 타당성 및 신뢰성을 미리 확보하기 위해 정보보안 관련 실무자들을 대상으로 인터뷰 및 파일럿 테스트를 실시하였다. 파일럿 테스트 결과, 본 연구모형에서 사용된 설문항목은 취약점 자기효능감 관련 5개 항목(시간 투자, 방법 도움, 사전 취약점 도구 이용 경험, 타인의 도움, 위급 시 도움 요청), 몰입 관련 5개 항목(흥분·자극, 주의 끌기, 시간 왜곡, 몰두), 인지된 이익 관련 5개 항목(금전적 이익, 명성, 해킹기술 역량향상, 지적호기심 충족, 주관적의미 부여), 화이트마켓 이용의도 관련 4개 항목(화이트마켓 취약점 가격 > 블랙마켓 취약점 가격, 화이트마켓 취약점 가격 = 블랙마켓 취약점 가격, 취약점 정보 문제해결 예상, 화이트마켓 법적제도 완비), 블랙마켓 이용의도 관련 3개 항목(블랙마켓 취약점 가

격 > 화이트마켓 취약점 가격, 취약점 정보 악용 예상, 법적 제도 부재)으로 구성하였다. 각 문항은 '1 = 매우 그렇지 않다', '2 = 그렇지 않다', '3 = 보통이다', '4 = 그렇다', '5 = 매우 그렇다'로 응답할 수 있는 5점 리커트 척도(Likert Scale)로 측정하였다.

〈표 6〉 본 연구의 설문문항 및 주요 참고문헌

연구변수	설문문항	주요 참고문헌
취약점 연구 자기효능감	취약점 분석 도구가 제공된 작업을 완료하는데 많은 시간이 주어진다면 취약점 분석 도구를 사용하여 작업을 완료할 수 있을 것이다.	Bandura(1982) Compeau and Higgins(1995) Giboney *et al.*(2016)
	누군가가 나에게 먼저 취약점 분석을 수행하는 방법을 보여준다면 취약점 분석 도구를 사용하여 작업을 완료할 수 있을 것이다.	
	같은 작업을 하기 전에 유사한 취약점 분석 도구를 이용한 경험이 있다면 취약점 분석 도구를 사용하여 작업을 완료할 수 있을 것이다.	
	누군가가 나에게 취약점 분석을 하는데 도움을 준다면 취약점 분석 도구를 사용하여 작업을 완료할 수 있을 것이다.	
	취약점 분석 작업이 막혔을 경우 내가 누군가에게 도움을 요청할 수 있다면 취약점 분석 도구를 사용하여 작업을 완료할 수 있을 것이다.	
몰입	보안 취약점을 발견하는 활동은 나를 흥분, 자극시킨다.	Csikzentmihalyi(1975) Voiskounsky and Smyslova(2003) 우형진(2004)
	보안 취약점의 발견은 나의 주의를 끈다.	
	나는 보안 취약점을 발견하는 활동을 하다 보면 다른 일을 잊곤 한다.	
	나는 보안 취약점을 연구하면서 몰입을 경험하곤 한다.	
인지된 이익	보안 취약점을 찾는 행위를 통해서 금전적 이익을 얻을 수 있다고 생각한다.	Algarni *et al.*(2014) Bugcrowd Inc.(2016) Young *et al.*(2007)
	보안 취약점을 찾는 행위를 통해서 명성을 얻을 수 있다고 생각한다.	
	보안 취약점을 찾는 행위를 통해서 해킹 기술을 자랑할 수 있다고 생각한다.	
	보안 취약점을 찾는 행위를 통해서 지적 호기심을 만족시킬 수 있다고 생각한다.	
	보안 취약점을 찾는 행위는 나에게 의미를 준다고 생각한다.	
화이트마켓 이용의도	암시장보다 합법적 시장에서 취약점 정보 가격이 더 비싸다면 나는 합법적 시장에서 취약점 정보를 거래할 의도가 있다.	Algarni *et al.*(2014) Egelman *et al.*(2013) Venkatesh *et al.*(2003)
	같은 가격에 취약점 정보가 거래된다면 나는 합법적 시장에서 거래할 의도가 있다.	
	합법적 시장에서 거래되는 취약점 정보는 소프트웨어의 문제 해결에 도움이 될 것으로 생각하기 때문에 나는 합법적 시장에서 취약점 정보를 거래할 의도가 있다.	
	취약점 정보를 거래할 수 있는 법적 제도가 생긴다면 나는 합법적 시장에서 취약점 정보를 거래할 생각이 있다.	
블랙마켓 이용의도	합법적 시장보다 암시장에서 취약점 정보 가격이 더 비싸다면 나는 암시장에서 취약점 정보를 거래할 의도가 있다.	Ablon *et al.*(2014) Egelman *et al.*(2013) Venkatesh *et al.*(2003)
	취약점 정보가 악용될 것으로 예상됨에 불구하고 암시장에서 거래할 의도가 있다.	
	취약점 정보를 거래할 수 있는 법적 제도가 없다면 나는 암시장에서 취약점 정보를 거래할 생각이 있다.	

Ⅴ. 실증분석

5.1 측정모형

본 연구에서는 PLS(Partial Least Squares) 분석을 하는 경우에 측정 문항과 구성개념에 대한 내적일관성(Internal Consistency), 집중타당성(Convergent Validity), 판별타당성(Discriminant Validity) 검정을 요구한다. 측정항목의 내적일관성 검정을 위해 보안 연구자의 취약점 연구 자기효능감, 몰입, 인지된 이익, 화이트마켓 이용의도, 블랙마켓 이용의도 요인을 대상으로 Fornell and Larcker (1981)의 복합신뢰도(Composite Reliability)와 신뢰성(Reliability)을 기준으로 검정하였다. 복합신뢰도는 Nunnally(1987)와 Thompson *et al.*(1995)이 주장하는 기준치인 0.7 이상으로 나타났고, 신뢰성 검정에 널리 사용되는 크론바하 알파(Cronbach's Alpha) 값은 기준치인 0.7 이상으로 나타났다. 따라서 본 연구모형은 높은 수준의 내적일관성을 보여준다(<표 7> 참조).

집중타당성은 AVE(Average Variance Extracted, AVE)와 요인 적재값(Factor Loading)의 t-값으로 검정하였다. AVE값은 Fornell and Larcker(1981), Chin(1998) 등이 주장하는 기준치인 0.5 이상으로 나타났다. 또한 구성개념에 적재된 요인적재량의 t-값은 1.96 이상으로 나타나 유의수준 5%에서 유의하였기 때문에 집중타당성이 있는 것으로 나타났다(<표 7> 참조).

판별타당성은 <표 8>과 같이 구성개념 간의 상관계수 값들의 대각선 축에 표시되는 AVE의 제곱근 값이 다른 구성개념 간의 상관계수 값보다 큰가의 여부로 검정한다(Fornell and Larcker, 1981). 검정결과, AVE의 제곱근 값 중 가장 작은 값 0.826이 가장 큰 상관계수 값 0.486을 상회하고 있으므로 본 연구모형의 구성개념은 판별타당성을 확보하였음을 확인하였다.

PLS 분석은 탐색적 요인분석(Exploratory Factor Analysis, EFA)보다는 확인적 요인분석(Confirmatory Factor Analysis, CFA)을 요구한다. 확인적 요인분석에서는 구성개념에 대한 요인 적재값이 다른 구성개념에 대한 요인 적재값 보다 커야 하는데, <표 9>에서 측정 문항의 교차 적재값(Cross Loadings)은

〈표 7〉 신뢰도 및 타당성 분석 결과

구 분	평균	AVE	크론바하 알파	복합신뢰도
취약점 연구 자기효능감	3.83	0.740	0.913	0.934
몰입	3.51	0.803	0.918	0.942
인지된 이익	3.71	0.683	0.883	0.915
화이트마켓 이용의도	3.65	0.794	0.912	0.939
블랙마켓 이용의도	2.48	0.790	0.869	0.919

〈표 8〉 판별타당성 분석 결과

구 분	취약점 연구 자기효능감	몰입	인지된 이익	화이트마켓 이용의도	블랙마켓 이용의도
취약점 연구 자기효능감	0.860				
몰입	0.376	0.896			
인지된 이익	0.324	**0.486**	**0.826**		
화이트마켓 이용의도	0.347	0.305	0.440	0.891	
블랙마켓 이용의도	-0.042	0.280	0.320	0.340	0.896

〈표 9〉 확인적 요인분석 분석 결과

구 분		취약점 연구 자기효능감	몰입	인지된 이익	화이트마켓 이용의도	블랙마켓 이용의도
취약점 연구 자기효능감	VRSF1	**0.822**	0.402	0.341	0.345	-0.043
	VRSF2	**0.852**	0.230	0.095	0.250	-0.203
	VRSF3	**0.855**	0.279	0.301	0.263	-0.107
	VRSF4	**0.875**	0.250	0.265	0.259	-0.192
	VRSF5	**0.895**	0.388	0.312	0.337	0.011
몰입	F1	0.292	**0.905**	0.443	0.284	0.208
	F2	0.320	**0.924**	0.508	0.297	0.244
	F3	0.430	**0.836**	0.301	0.216	0.149
	F4	0.318	**0.917**	0.473	0.286	0.244
인지된 이익	PB1	0.200	0.212	**0.714**	0.364	0.318
	PB2	0.302	0.401	**0.832**	0.466	0.257
	PB3	0.395	0.447	**0.875**	0.260	0.109
	PB4	0.234	0.377	**0.849**	0.379	0.198
	PB5	0.203	0.544	**0.853**	0.328	0.215
화이트마켓 이용의도	WMBI1	0.302	0.332	0.324	**0.874**	0.233
	WMBI2	0.343	0.343	0.433	**0.911**	0.217
	WMBI3	0.323	0.263	0.355	**0.950**	0.189
	WMBI4	0.261	0.142	0.438	**0.824**	0.120
블랙마켓 이용의도	BMBI1	-0.044	0.208	0.309	0.275	**0.891**
	BMBI2	-0.165	0.216	0.043	0.118	**0.887**
	BMBI3	-0.098	0.215	0.303	0.162	**0.889**

기준치인 0.7 이상이고 다른 구성개념에 대한 모든 요인 적재값 보다 크기 때문에, 모든 설문문항이 본 요건을 충족하였다.

본 연구의 연구모형에서 사용된 측정 문항과 구성 개념에 대한 내적일관성, 집중타당성, 판별타당성을 검정한 결과 모든 기준 요건을 만족하였다. 따라서 본 연구에서 제시한 연구모형의 신뢰성과 타당성을 확인하였다.

5.2 연구모형 및 가설검정 결과

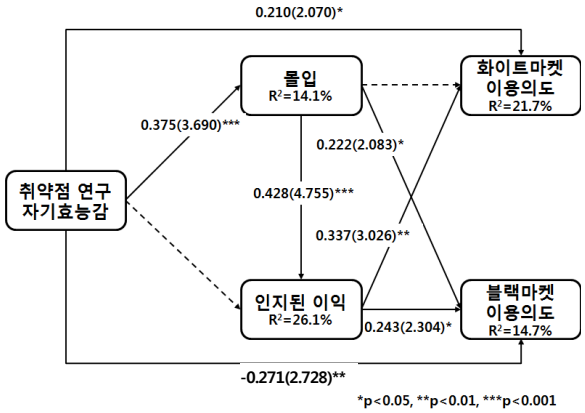
본 연구에서 제시된 연구모형 분석을 위한 소프트웨어로 Smart PLS 2.0을 사용하였으며 부트스트랩 리샘플링(Bootstrap Resampling)기법으로 리샘플링을 5,000회 한 후에 분석하였다(Hair *et al.*, 2016).

본 연구에서는 연구모형의 적합도 검정을 실시하기 위한 기준으로 R^2값, Redundancy값, GoF값을 사용하였다. PLS 분석에서 경로모형의 설명력은 결정계수(Explained Variance) R^2값을 예측적합도 지수로 사용하며 평가한다(Chin and Gopal, 1995). 이상의 목적을 위해 본 연구에서는 Cohen(1988)과 Falk and Miller(1992)가 제시한 R^2값으로 본 연구모형의 적합도를 평가하였다. R^2 분석결과, 본 연구의 몰입의 결정계수 R^2값은 0.140이므로 중간정도인 것으로 나타났으며 인지된 이익의 결정계수 R^2값은 0.260이므로 0.26 이상이므로 높은 것으로 나타났다. 또한 화이트마켓 이용의도의 결정계수

〈표 10〉 본 연구의 연구가설 검정결과

구 분	경로	상관계수	t-값	결과
H1-1	취약점 연구 자기효능감 → 몰입	0.375	3.725***	채택
H1-2	취약점 연구 자기효능감 → 인지된 이익	0.163	1.544	기각
H1-3	취약점 연구 자기효능감 → 화이트마켓 이용의도	0.215	2.246*	채택
H1-4	취약점 연구 자기효능감 → 블랙마켓 이용의도	-0.271	2.797**	채택
H2-1	몰입 → 인지된 이익	0.426	4.789***	채택
H2-2	몰입 → 화이트마켓 이용의도	0.057	0.826	기각
H2-3	몰입 → 블랙마켓 이용의도	0.222	2.040*	채택
H3-1	인지된 이익 → 화이트마켓 이용의도	0.342	3.062**	채택
H3-2	인지된 이익 → 블랙마켓 이용의도	0.244	2.328*	채택

*p < 0.05, **p < 0.01, ***p < 0.001.



〈그림 3〉 본 연구의 경로계수

R^2값은 0.242, 블랙마켓 이용의도의 결정계수 R^2 값은 0.147로 중간정도인 것으로 나타났다(0.26 이상 = 상, 0.13~0.26 = 중, 0.02~0.13 = 하). 그리고 모든 요인들의 R^2값이 Falk and Miller(1992)가 제시한 적정 검정력 0.1을 상회하며 또한 Redundancy 값도 양수로 나타나 연구모형의 적합도가 높다고 판단된다.

최근에는 PLS 경로 모형의 적합도 검정(Goodness-of-Fit, GoF)를 권장하고 있다(Tenehaus *et al.*, 2005; Wetzels *et al.*, 2009). 이에 따라 본 연구에서는 GoF 검정 기준으로 공통성(Communality) 평균과 R^2 평균의 기하평균을 사용하였다. 분석결과 GoF 영향도 값은 0.388이므로 Wetzels *et al.*(2009)이 제시한 값[2]보다 크기 때문에 본 연구에서 사용된 모형에 대한 전체적 적합도가 높다고 판단된다.

다음으로 본 연구의 가설을 검정하기 위하여 경로계수의 유의성을 검정하였다. 이를 위하여 전체표본에 대한 구조모형의 경로계수를 구한 뒤 Smart PLS 2.0 프로그램에서 제공하는 부트스트랩(Bootstrap)분석을 통하여 t-값을 구하였다.

본 연구의 가설은 <표 10>, <그림 3>에서 보는 바와 같이 첫째, 보안 연구자의 취약점 연구 자기효능감이 영향을 미치는 4가지 요인 중에서 몰입

2) Wetzels *et al.*(2009)에 따르면 GoF의 영향도는 0.1, 0.25, 0.36을 기준으로 각각 약(small), 중(medium), 강(large)으로 분류하였다.

(β = 0.375, tβ = 3.725, p < 0.001), 화이트마켓 이용의도(β = 0.215, t = 2.246, p < 0.05), 블랙마켓 이용의도(β = -0.271, t = 2.797, p < 0.01)가 유의한 것으로 나타났다. 따라서 H1-1, H1-3, H1-4가 채택되었다. 그러나 인지된 이익(β = 0.163, t = 1.544, p > 0.05)은 유의하지 않은 것으로 나타나 H1-2가 기각되었다. 둘째, 보안 연구자의 몰입이 영향을 미치는 세 가지 요인 중에서 인지된 이익(β = 0.426, t = 4.789, p < 0.001), 블랙마켓 이용의도(β = 0.222, t = 2.040, p < 0.05)가 유의한 것으로 나타났다. 따라서 H2-1, H2-3이 채택되었다. 그러나 화이트마켓 이용의도(β = 0.057, t = 0.826, p > 0.05)는 유의하지 않은 것으로 나타나 H2-2가 기각되었다. 셋째, 보안 연구자의 인지된 이익이 취약점마켓 이용의도에 영향을 미치는 요인 중에서 화이트마켓 이용의도(β = 0.342, t = 3.062, p < 0.01), 블랙마켓 이용의도(β = 0.244, t = 2.328, p < 0.05)가 유의한 것으로 나타났다. 따라서 H3-1, H3-2가 채택되었다.

5.3 연구결과의 논의

본 연구는 보안 취약점 연구동기(취약점 연구 자기효능감, 몰입, 인지된 이익)와 취약점마켓 이용의도(화이트마켓 이용의도, 블랙마켓 이용의도)에 영향을 미치는 요인으로 구분한 후 연구모형을 만들어 구조방정식 분석을 실시하였다. 본 연구에서 제시된 연구모형을 취약점 분석 경험이 있는 보안 연구자들을 대상으로 실증분석 한 결과는 다음과 같다. 취약점 연구 자기효능감은 몰입, 화이트마켓 이용의도, 블랙마켓 이용의도에 영향을 미쳤고, 몰입은 인지된 이익과 블랙마켓 이용의도에 영향을 미쳤으며, 인지된 이익은 화이트마켓 이용의도, 블랙마켓 이용의도에 유의한 영향을 미치는 것으로 확인되었다.

5.3.1 취약점 연구 자기효능감

취약점 연구 자기효능감은 몰입에 유의한 영향을 미친다. <표 7>을 살펴보면 보안 연구자의 취약점 연구 자기효능감 평균값 3.83[3]으로 나타나 보안 연구자는 취약점 연구 자기효능감을 지각하고 있는 것을 알 수 있다. 가설검정 결과, 취약점 연구 자기효능감은 몰입에 영향을 미치는 것으로 나타났다(β = 0.375, t = 3.725). 이는 본 연구모형에 대한 선행연구결과와 동일하게 취약점 연구 자기효능감이 몰입에 유의한 영향을 미친다는 것을 재차 입증한 연구 결과이다(Voiskounsky and Smyslova, 2003; 김기병 등, 2015; 박상호, 2011; 배현숙, 2015). 즉, 취약점 연구를 수행하면서 시간 투자, 방법 도움, 사전 취약점 도구 이용 경험, 타인의 도움, 위급 시 도움 요청과 같은 취약점 연구 자기효능감을 인지하는 보안 연구자는 취약점 연구를 통해 몰입을 경험할 것이다.

취약점 연구 자기효능감은 인지된 이익에 유의한 영향을 미치지 않는다. 가설검정 결과, 취약점 연구 자기효능감은 인지된 이익에 유의한 영향을 미치지 않은 것으로 나타났다(β = 0.163, t = 1.544). 본 연구모형에 대한 선행연구결과와 달리 취약점 연구 자기효능감이 인지된 이익에 유의한 영향을 미치지 않는다는 것을 확인한 연구 결과이다(Giboney *et al*., 2016; 김용일, 양현교, 2012; 성행남, 2014). 이를 통해 보안 연구자는 취약점 연구에 대해 시간 투자, 방법 도움, 사전 취약점 도구 이용 경험, 타인의 도움, 위급 시 도움 요청과 같은 취약점 연구 자기효능감을 갖지만 실제 인지된 이익에는 영향을 미치지 않는다는 것을 확인하였다.

취약점 연구 자기효능감은 화이트마켓과 블랙마켓 이용의도에 유의한 영향을 미친다. 보안 연구자의 화이트마켓 이용의도 평균값이 3.65로 나타나 보안 연구자는 화이트마켓 이용의도를 갖고 있음을 알 수 있다. 반면에 블랙마켓 이용의도 평

3) 각 문항은 '1. 전혀 그렇지 않다, 2. 그렇지 않다, 3. 보통이다, 4. 그렇다, 5. 매우 그렇다'라는 항목으로 5점 리커트 척도(Likert Scale)로 측정하였다. 일반적으로 평균값이 3.00 이상이면 '그렇다', 3.00 미만이면 '그렇지 않다'라고 해석할 수 있다.

균값은 2.48로 나타나 보안 연구자는 블랙마켓 이용의도를 갖고 있지 않음을 알 수 있다. 가설검정 결과, 취약점 연구 자기효능감은 화이트마켓과 블랙마켓 이용의도에 유의한 영향을 미치는 것으로 확인되었다(β = 0.215, t = 2.246)(β = -0.271, t = 2.797). 이는 본 연구모형에 대한 선행연구결과와 동일하게 취약점 연구 자기효능감이 취약점마켓 이용의도에 유의한 영향을 미친다는 것을 재차 입증한 연구 결과이다(Ablon *et al*., 2014; Algarni *et al*., 2014; Chau, 2001; Egelman *et al*., 2013; Venkatesh *et al*., 2003). 여기서 주목할 점은 취약점 연구 자기효능감이 블랙마켓 이용의도에 직접적으로 부(-)의 영향을 갖지만 몰입과 인지된 이익이 각각 매개된 경로에서는 지속적으로 정(+)의 영향을 미치는 점이다. 이는 보안 연구자가 취약점 연구 자기효능감 요인만으로는 블랙마켓에 이용의도에 부정적이며 취약점 연구 자기효능감을 충족시킨 후 취약점 연구에 몰입하거나 취약점 연구에 대한 이익을 인지하여 블랙마켓 이용의도에 긍정적으로 생각하는 것으로 해석된다.

5.3.2 몰입

몰입은 인지된 이익에 유의한 영향을 미친다. 보안 연구자의 몰입은 평균값이 3.51로 나타나 보안 연구자는 취약점을 연구하면서 몰입을 경험하는 것을 알 수 있다. 가설검정 결과, 몰입은 인지된 이익에 영향을 미치는 것으로 나타났다(β = 0.426, t = 4.789). 이는 선행연구에서 도출한 보안 연구자의 몰입이 인지된 이익에 유의한 영향을 미친다는 것을 입증한 연구 결과이다(Beveren, 2001; Voiskounsky and Smyslova, 2003; 박찬현 등, 2016; 우형진, 2004). 즉, 보안 연구자는 취약점을 발견하는 행위를 통해서 흥분과 자극을 느끼며, 연구자의 주의를 끌고, 다른 일을 잊어버리며, 몰두하는 경향이 있다. 이러한 보안 취약점 연구에 몰입을 경험하는 보안 연구자는 보안 취약점 연구를 통해 이익을 얻는 것을 기대할 것이다. 특히 본 연구의 응답자는 취약점 분석경험(응답자의 100%), 모의해킹 업무경험(62.3%)을 갖고 있으며 해킹기술을 습득하기 위하여 커뮤니티 활동(61%), 교육기관(57.1%), 컨퍼런스(39%), 해킹대회(31.2%), SNS(27.3%) 이용을 하고 해킹기술을 실습하기 위하여 가상환경(80.5%), 허가된 시스템(58.4%), 워게임(48.1%), 해킹대회(33.8%) 참여와 같은 활동을 통하여 보안 취약점 연구 역량을 높이기 위하여 적극적으로 노력하는 경향이 있다. 따라서 취약점 연구를 통해 몰입을 경험하는 보안 연구자는 취약점 연구에 대한 이익을 기대하고 있음을 알 수 있다.

몰입은 화이트마켓 이용의도에 유의한 영향을 미치지 않으며 블랙마켓 이용의도에 유의한 영향을 미친다. 가설검정 결과, 몰입은 화이트마켓 이용의도에 영향을 미치는 않는 것으로 나타났고(β = 0.057, t = 0.826), 블랙마켓 이용의도에 영향을 미치는 것으로 나타났다(β = 0.222, t = 2.040). 이러한 결과는 선행연구를 토대로 도출된 몰입과 취약점마켓 이용의도 가설을 모두 충족시키지 못한 것을 알 수 있다(Ablon *et al*., 2014; Algarni *et al*., 2014; Egelman *et al*., 2013; Voiskounsky and Smyslova, 2003; 박신영, 2013;, 박찬현 등, 2016; 우형진, 2004; 이현지, 정동훈, 2012;, 진경미, 장순자, 2016; 허지현, 2013). 이는 보안 연구자의 몰입이 화이트마켓 이용의도에는 유의한 영향을 미치지만, 블랙마켓 이용의도에는 유의한 영향을 미치지 않는 것을 확인한 연구결과이다.

5.3.3 인지된 이익

인지된 이익은 취약점 연구 자기효능감은 화이트마켓과 블랙마켓 이용의도에 유의한 영향을 미친다. 보안 연구자의 인지된 이익은 평균값이 3.71로 나타나 보안 연구자는 취약점 연구를 통해 인지된 이익을 지각하는 것을 알 수 있다. 가설검정 결과, 인지된 이익은 화이트마켓 이용의도에 영향을 미치는 것으로 나타났고(β = 0.342, t = 3.062), 블랙마켓 이용의도에 영향을 미치는 것으로 나타났다(β = 0.244, t = 2.328). 이는 취약점마켓

참여자와 해커에 대한 연구에서 제시된 취약점 연구를 통한 보안 연구자의 인지된 이익이 화이트마켓 이용의도와 블랙마켓 이용의도 모두 유의한 영향을 미친다는 것을 입증한 연구 결과이다(Algarni *et al*., 2013, 2014; Finifter *et al*., 2013; Giboney *et al*., 2016; Owen, 2016; Zaho *et al*., 2014). 즉, 보안 연구자는 취약점을 찾는 행위를 통해서 금전적 이익, 명성, 해킹기술 역량 향상, 지적 호기심 충족, 의미부여와 같은 인지된 이익을 느낀다. 따라서 보안 연구자들은 취약점 정보 거래 시장인 화이트마켓, 블랙마켓에서 적절한 보상을 제공한다면 이용하게 될 가능성이 높을 것이다.

Ⅵ. 결 론

6.1 연구결과의 요약

보안 위협으로부터 정보시스템의 자산을 지키기 위한 방법 중 하나로 보안 취약점 정보 거래를 할 수 있는 취약점마켓이 생겼으며 그 종류와 범위가 확대되고 있다. 본 연구는 취약점 분석이 실무를 수행할 수 있는 보안 연구자들을 대상으로 취약점을 연구하는 동기가 무엇인가? 취약점마켓 이용의도에 영향을 미치는 것은 무엇인가? 에 대한 질문으로부터 시작되었다. 이러한 질문을 시작으로 본 연구에서는 취약점마켓과 해커와 관련된 선행연구를 통하여 보안 연구자의 연구행위에 영향을 미치는 요인으로 취약점 연구 자기효능감, 몰입, 인지된 이익 요인을 도출하였고, 취약점마켓 이용의도인 화이트마켓 이용의도, 블랙마켓 이용의도를 도출하였다.

본 연구에서는 취약점 분석경험이 있는 사람을 대상으로 154부의 유효한 설문지를 회수한 후, 통계분석 소프트웨어인 Smart PLS 2.0을 활용하여 보안 연구자의 연구행위와 취약점마켓 이용의도 간의 인과관계를 분석하였다. 분석결과, 첫째, 취약점 연구 자기효능감은 몰입, 블랙마켓 이용의도, 화이트마켓 이용의도 순으로 유의한 영향을 미치고 있는 것으로 나타났다. 둘째, 보안 연구자의 몰입은 인지된 이익과 블랙마켓 이용의도에 유의한 영향을 미치는 것으로 나타났다. 셋째, 보안 연구자의 인지된 이익은 화이트마켓 이용의도와 블랙마켓 이용의도 모두에 유의한 영향을 미치는 것으로 확인되었다. 넷째, 취약점 연구 자기효능감은 몰입을 매개로 인지된 이익에 유의한 영향을 미치는 것으로 확인되었다. 마지막으로 몰입은 인지된 이익을 매개로 화이트마켓 이용의도와 블랙마켓 이용의도에 모두 유의한 영향을 미치는 것으로 확인되었다. 하지만 예상과 달리 보안 연구자의 취약점 연구 자기효능감은 인지된 이익에 유의한 영향을 미치지 않았고 몰입은 화이트마켓 이용의도에 유의한 영향을 미치지 못하는 것으로 나타났다.

6.2 연구의 시사점

6.2.1 이론적 시사점

보안 취약점 연구 대부분 기술적 측면에 초점이 맞춰져 있고 정보보호 행동 연구에서도 일반인을 대상으로 특정 서비스(클라우드 서비스, 스마트폰 등)에 대한 정보보호 효과에 대한 요인을 규명하는데 집중하였다. 본 연구에서는 취약점 분석 경험이 있는 보안 연구자들을 대상으로 취약점 연구동기와 취약점 정보를 거래할 수 있는 마켓(화이트마켓, 블랙마켓) 이용의도에 대하여 실증분석 하였다는데 의의가 있다. 본 연구에서 주목할 만한 연구결과는 다음과 같다.

첫째, 사람의 행동을 예측하는데 여러 분야에 이용된 사회인지이론과 플로우이론을 토대로 지금까지 진행된 사례가 없는 보안 연구자의 취약점 연구 동기에 관한 연구모형을 제시하고 실증한 것이다. 이에 본 연구모형의 제시는 보안 연구자의 취약점 연구 동기에 대한 좀 더 풍부한 설명을 제시할 수 있는 이론적 기반이 될 것으로 기대한다. 둘째, 본 연구에서 제시한 취약점 연구 자기효능

감 요인이 몰입에 유의한 영향을 미치고 인지된 이익에는 유의한 영향이 없다는 결과를 도출한 것이다. 즉, 취약점 연구 자기효능감을 느끼는 사람은 바로 이익을 인지하지 않지만 취약점 연구에 대한 몰입 경험을 한다면 이익을 인지한다는 연구결과를 제ㄷ출하였다. 셋째, 보안 연구자의 몰입 경험이 인지된 이익에 가장 높은 영향을 미친다는 것을 확인하였다. 이는 보안 연구자가 취약점 연구에 대하여 몰입을 경험할수록 보안 취약점 정보에 대하여 얻을 수 있는 이익의 가치를 더욱 높게 인식하는 것으로 해석된다. 넷째, 인지된 이익이 화이트마켓 이용의도와 블랙마켓 이용의도에 모두 유의한 영향을 미친다는 것을 확인한 것이다. 이 결과는 보안 취약점 연구를 통해 보안 취약점 정보에 대한 가치 및 이익을 인지한 보안 연구자들이 취약점을 거래할 수 있는 시장이 마련된다면 거래할 의사가 있다는 것을 확인한 것이다. 다섯째, 취약점 연구 자기효능감이 블랙마켓 이용의도에 직접적으로 부(-)의 영향을 갖지만 몰입과 인지된 이익이 각각 매개된 경로에서는 지속적으로 정(+)의 영향을 미치는 점이다. 이는 보안 연구자가 취약점 연구 자기효능감 요인만으로는 블랙마켓에 이용의도에 부정적이며 취약점 연구 자기효능감을 충족시킨 후 취약점 연구에 몰입하거나 취약점 연구에 대한 이익을 인지하여 블랙마켓 이용의도에 긍정적으로 생각하는 것으로 해석된다.

6.2.2 실무적 시사점

본 연구는 실제 취약점 분석 경험이 있는 보안 연구자들을 대상으로 진행하였다. 따라서 본 연구의 결과가 보안 연구자에 대한 행태적 연구 및 한국형 취약점마켓을 설계하기 위한 실무적 도움이 될 만한 여지가 있다고 판단된다. 본 연구에서 실무적으로 주목할 만한 연구결과는 다음과 같다.

첫째, 본 연구에서는 취약점 분석 도구를 이용한 경험이 있는 표본을 확보하여 연구를 진행하였다. 인구통계학적 분석결과, 보안 연구자는 주로 커뮤니티 활동 및 교육기관을 통해 해킹기술을 습득하고 가상환경과 허가된 시스템 그리고 워게임을 통하여 해킹기술을 실습하는 것을 확인하였다. 둘째, 취약점마켓 이용의도를 화이트마켓 이용의도와 블랙마켓 이용의도로 구분하여 가격, 취약점 이용, 법적제도유무에 대한 기준으로 측정하였다. 아직 국내 보안 연구자에게 취약점마켓이란 용어를 질의하면 한국인터넷진흥원에서 운영하는 'S/W 취약점 신고 포상제도'를 떠올리며 또한 생소하기 때문에 취약점마켓에 대한 선행연구를 토대로 취약점마켓을 구분한 특징들을 토대로 설문문항을 만들어 측정하였다. 셋째, 현 시점까지 진행된 취약점마켓의 종류, 정의 및 연구 현황을 정리하였다. 따라서 본 연구에서 정리된 취약점마켓의 종류 및 현황을 참고하여 보안 연구자에게 보안 취약점 정보에 대한 가치 및 이익을 인식하는 계기가 되기를 기대한다.

6.3 연구의 한계 및 향후 연구 방향

본 연구에서는 보안 연구자의 취약점 연구동기와 취약점마켓 이용의도에 초점을 맞추어 연구모형을 제시하였고 가설을 검정하였다. 하지만 본 연구를 진행함에 있어 현실적인 제약으로 인하여 미처 고려하지 못한 한계점이 있었으며 이에 대한 향후 연구 방향을 제시하였다.

첫째, 연구의 표본을 보안 연구자 즉, 화이트해커로 한정하여 설문지 배포 및 분석을 진행하였다. 미디어 및 사회에서 다뤄지는 해커 및 취약점 분석에 대한 좋지 않은 인식으로 인하여 블랙 해커를 만나기 힘들기 때문에 악의적인 목적을 가진 보안 연구자에 대한 설문 응답을 받는 것이 용이하지 않았다. 이러한 문제점을 해결하기 위하여 향후 연구에서는 해외의 보안 커뮤니티 및 다크 웹(Dark Web)에 접속하여 설문지를 확보하여 블랙 해커를 대상으로 행태적 연구를 진행할 것이다.

둘째, 취약점 정보의 가격에 대하여 충분히 고려하지 못했다. 본 연구는 보안 연구자의 행동 예

측을 위한 초기 연구이다. 따라서 취약점마켓과 해커에 대한 선행연구에서 도출한 인지된 이익이란 측정항목을 개발하였고 이에 대한 신뢰도와 타당도를 확보하였다. 향후 취약점마켓에서 거래되는 취약점 정보의 중요도와 심각성 수준을 고려한 실질적 요인(예: 금전적 인센티브 등), 쾌락적 요인(예: 재미, 즐거움 등)에 대한 측정 도구를 개발하여 연구를 진행할 것이다.

셋째, 몰입의 측정 기준을 개인의 몰입 성향으로 한정하였다. 본 연구의 설계 시점에 국내 취약점마켓이 구체적인 형태로 드러나 있지 않아 몰입의 측정 기준을 특정 사이트 및 마켓을 구분하지 않았다. 그러나 2017년 9월 현재 삼성에서 스마트폰 및 서비스에 관한 보안 취약점을 제보한 사람에게 최소 200달러에서 최대 20만 달러를 지급하는 버그 바운티를 실시함에 따라 취약점마켓에 대한 보안 연구자들에 대한 수요가 증가할 것으로 예상된다. 이에 취약점마켓의 수요가 증가하여 시장과 보안 연구자들의 관심이 증가되면 향후 취약점마켓의 종류와 성격에 대한 구체적인 비교연구를 수행할 수 있는 토대가 마련될 것이다.

넷째, 취약점마켓 이용의도의 선행요인을 제한적(취약점 연구 자기효능감, 몰입, 인지된 이익)으로 접근하여 도덕 및 윤리와 같은 내부 요인을 설명하지 못하였다. 후속 연구에선 취약점 정보 활용에 개인적 심리와 도덕적 요인이 취약점마켓 이용의도에 끼치는 영향을 설명할 수 있는 접근이 필요하다.

참 고 문 헌

[1] 김기병, 봉미희, 서원석, “자기효능감이 관광몰입과 관광 만족에 미치는 영향”, *관광·레저연구*, 제27권, 제2호, 2015, pp. 365-386.

[2] 김민정, 유진호, “S/W 취약점으로 인한 손실비용 추정”, *한국전자거래학회지*, 제19권, 제44호, 2014, pp. 31-43.

[3] 김용일, 양현교, “정보시스템 수용자의 컴퓨터 자기효능감, 정보시스템 품질, 수용태도와 업무성과 간의 구조적 관계에 관한 연구”, *관광연구*, 제27권, 제2호, 2012, pp. 75-93.

[4] 미하이 칙센트미하이, *몰입의 경영*, ㈜황금가지, 서울, 2006.

[5] 박상호, “인터넷 이용동기가 인터넷 자기효능감, 인터넷 몰입과 인터넷 중독에 미치는 영향에 관한 연구”, *정치커뮤니케이션 연구*, 제22호, 2011, pp. 37-80.

[6] 박신영, “스마트폰 사용자의 이용 동기와 이용 정도에 따른 플로우 경험”, *방송통신연구*, 제81호, 2013, pp. 97-126.

[7] 박찬현, 송인욱, 김민지, 장은희, 허준, 김현택, “해커들의 심리변인에 기반한 탈선적 해킹활동 및 해킹타입 예측 모델”, *한국통신학회논문지*, 제41권, 제4호, 2016, pp. 489-498.

[8] 배현숙, “항공사 객실승무원의 개인특성이 팀 웍 및 팀만족, 조직몰입에 미치는 영향”, *관광레저연구*, 제27권, 제12호, 2015, pp. 355-374.

[9] 성행남, 신재익, “모바일 학습에서 자기효능감이 행동의도에 미치는 영향에 관한 연구: 촉진조건의 조절효과를 중심으로”, *인터넷전자상거래연구*, 제15권, 제4호, 2015, pp. 349-364.

[10] 우종필, *구조방정식모델 오해와 편견*, 한나래출판사, 서울, 2014.

[11] 우형진, “해커의 심리변인이 해킹행위에 미치는 영향에 관한 연구”, *한국언론학보*, 제48권, 제3호, 2004, pp. 90-115.

[12] 이현지, 정동훈, “스마트폰 게임센서에 따른 상호작용성과 플로우, 태도 그리고 이용의도에 관한 연구”, *한국방송학보*, 제26권, 제1호, 2012, pp. 126-166.

[13] 장재영, 김범수, “동기적, 사회적, 그리고 환경적 요인이 해커의 기술 습득에 미치는 영향”, *Information Systems Review*, 제18권, 제1호, 2016, pp. 57-78.

[14] 진경미, 장순자, “계획된 행동과 Flow 경험에

따른 항공사 모바일 앱 이용의도 연구", *관광연구*, 제31권, 제4호, 2016, pp. 325-344.

[15] 한국인터넷진흥원, "S/W신규 취약점", 2016, Available at https://www.krcert.or.kr/consult/software/vulnerability.do?orgSiteUrl=http://www.krcert.or.kr.

[16] 허지현, "온라인 여행커뮤니티 이용동기와 플로우(flow) 경험 및 지속적 이용의도에 관한 연구", *관광연구*, 제28권, 제2호, 2013, pp. 161-181.

[17] A3Security, *크래커 잡는 명탐정 해커*, 성안당, 파주, 2010.

[18] Ablon, L., M. C. Libicki, and A. A. Golay, *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*, Rand Corporation, Santa Monica, CA, 2014.

[19] Algarni, A. and Y. Malaiya, "Most successful vulnerability discoverers: Motivation and methods", In *Proceedings of the International Conference on Security and Management* (SAM), 2013, pp. 1-7.

[20] Algarni, A. and Y. Malaiya, "Software vulnerability markets: Discoverers and buyers", *International Journal of Computer, Information Science and Engineering*, Vol.8, No.3, 2014, pp. 71-81.

[21] Andy, G., "Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits", 2012, Available at http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/#1d95627b6033.

[22] Arora, A., R. Krishnan, R. Telang, and Y. Yang, "An empirical analysis of software vendors' patch release behavior: Impact of vulnerability disclosure", *Information Systems Research*, Vol.21, No.1, 2010, pp. 115-132.

[23] Bambauer, D. E. and O. Day, "Hacker's aegis, the," *Emory Law Journal*, Vol.60, No.5, 2011, pp. 1051-1107.

[24] Bandura, A., "Self-efficacy mechanism in human agency", *American Psychologist*, Vol.37, No.2, 1982, pp. 122-147.

[25] Bandura, A., "Self-regulation of motivation through anticipatory and self-reactive mechanisms", In *Perspectives on Motivation: Nebraska Symposium on Motivation*, Vol.38, 1991, pp. 69-164.

[26] Barclay, D., C. Higgins, and R. Thompson, "The partial least squares (PLS) approach to causal modeling: Personal computer adoption and use as an illustration", *Technology Studies*, Vol.2, No.2, 1995, pp. 285-309.

[27] Beebe, N. L. and J. Guynes, "A model for predicting hacker behavior," *AMCIS 2006 Proceedings*, 2006, pp. 3394-3404.

[28] Beveren, J. V., "A conceptual model for hacker development and motivations", *Journal of E-Business*, Vol.1, No.2, 2001, pp. 1-9.

[29] Böhme, R., "Vulnerability markets: What is the economic value of a zero-day exploit?", *Proc. of 22C3: Private Investigations*, Berlin, 2005.

[30] Campbell, K., L. A. Gordon, M. P. Loeb, and L. Zhou, "The economic cost of publicly announced information security breaches: Empirical evidence from the stock market", *Journal of Computer Security*, Vol.11, No.3, 2003, pp. 431-448.

[31] Chan, S. H. and L. J. Yao, "An empirical investigation of hacking behavior", *Review of Business Information Systems (RBIS)*, Vol.9, No.4, 2011, pp. 41-58.

[32] Chau, P. Y. and P. J. H. Hu, "Information technology acceptance by individual professionals: A model comparison approach", *Decision Sciences*, Vol.32, No.4, 2001, pp. 699-719.

[33] Chin, W. W. and A. Gopal, "Adoption intention

in GSS: Relative importance of beliefs", *ACM SIGMIS Database*, Vol.26, No.2-3, 1995, pp. 42-64.

[34] Chin, W. W., "The partial least squares approach to structural equation modeling", *Modern Methods for Business Research*, Vol.295, No.2, 1988, pp. 295-336.

[35] Cohen, J. O., *Statistical Power Analysis for the Behavioral Sciences*, Lawrence Erlbaum, Hillsdale, NY, 1988.

[36] Compeau, D. R. and C. A. Higgins, "Computer self-efficacy: Development of a measure and initial test", *MIS Quarterly*, Vol.19, No.2, 1995, pp. 189-211.

[37] Csikszentmihalyi, M., *Beyond Boredom and Anxiety: The Experience of Play in Work and Game*, Jossey-Bass, San Francisco, CA, 2000.

[38] Egelman, S., C. Herley, and P. C. Van Oorschot, "Markets for zero-day exploits: Ethics and implications", In *Proceedings of the 2013 Workshop on New Security Paradigms Workshop*, ACM, 2013, pp. 41-46.

[39] Falk R. F. and N. B. Miller, *A Primer for Soft Modeling*, University of Akron Press, Ohio, OH, 1992.

[40] Fidler, M., *Anarchy or Regulation: Controlling The Global Trade in Zero-Day Vulnerabilities* (Doctoral dissertation), Stanford University, 2014.

[41] Finifter, M., D. Akhawe, and D. Wagner, "An empirical study of vulnerability rewards programs", In *Presented as Part of the 22nd USENIX Security Symposium*, 2013, pp. 273-288.

[42] Fitch, C., "Crime and punishment: the psychology of hacking in the new millennium", *Global Information Assurance Certification Paper*, GSEC Practical Requirements 1, 2004.

[43] Fornell, C. and D. Larcker, "Evaluating structural equation models with unobservable variables and measurement error", *Journal of Marketing Research*, Vol.18, No.1, 1981, pp. 39-50.

[44] Gefen, D., E. Karahanna, and D. W. Straub, "Trust and TAM in online shopping: An integrated model", *MIS Quarterly*, Vol.27, No.1, 2003, pp. 51-90.

[45] Giboney, J. S., J. G. Proudfoot, S. Goel, and J. S. Valacich, "The security expertise assessment measure(SEAM): Developing a scale for hacker expertise", *Computers and Security*, Vol.60, 2016, pp. 37-51.

[46] Ha, I., Y. Yoon, and M. Choi, "Determinants of adoption of mobile games under mobile broadband wireless access environment", *Information and Management*, Vol.44, No.3, 2007, pp. 276-286.

[47] Hair Jr, J. F., G. T. M. Hult, C. Ringle, and M. Sarstedt, *PLS 구조모델의 이해Basic-*, 피엔씨미디어, 고양, 2016.

[48] Hewlett Packard Enterprise, "The Vulnerability Market Decoded", 2014, Available at https://www.hpe.com/h20195/v2/GetPDF.aspx/4AA6-4175ENW.pdf.

[49] Hsu, C. L. and H. P. Lu, "Why do people play on-line games? An extended tam with social influences and flow experience", *Information and Management*, Vol.41, No.7, 2004, pp. 853-868.

Kesan, J. P. and C. M. Hayes, "Bugs in the market: Creating a legitimate, transparent, and vendor-focused market for software vulnerabilities", *Arizona Law Review*, Vol.58, No.16-18, 2016, pp. 753-830.

[50] Lent, R. W., S. D. Brown, and K. C. Larkin, "Relation of self-efficacy expectations to academic achievement and persistence," *Journal of Counseling Psychology*, Vol.31, No.3, 1984, pp. 356-362.

[51] Locke, E. A. and G. P. Latham, *A Theory of*

Goal Setting and Task Performance, Prentice Hall, Eaglewood Cliffs, NJ, 1990.

[52] Mitchell, R. J., "Path Analysis," in S. M. Scheiner and J. Gurevitch (eds.) *Design and Analysis of Ecological Experiments*, Oxford University Press, Oxford, 2001, 217-234.

[53] Nizovtsev, D. and M. Thursby, "Economic analysis of incentives to disclose software vulnerabilities," In *WEIS*, 2005, pp. 1-32.

[54] Novak, T. P., D. L. Hoffman, and A. Duhachek, "The influence of goal-directed and experiential activities on online flow experiences", *Journal of Consumer Psychology*, Vol.13, No.1, 2003, pp. 3-16.

[55] Nunnally, J. C., *Psychometric Theory*, McGrow-Hill, New York, NY, 1987.

[56] Owen, K., *Motivation and Demotivation of Hackers in the Selection of a Hacking Task: A Contextual Approach* (Doctoral dissertation), McMaster University, 2016.

[57] Stevens, J. P., Applied Multivariate Statistics for the Social Sciences, Routledge, New York, NY, 2012.

[58] Telang, R. and W. Sunil, "Impact of Software Vulnerability Announcements on the Market Value of Software Vendors-an Empirical Investigation", 2005, Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=677427.

[59] Tenenhaus, M., V. E. Vinzi, Y. M. Chatelin, and C. Lauro, "PLS path modeling", *Computational Statistics and Data Analysis*, Vol.48, No.1, 2005, pp. 159-205.

[60] Venkatesh, V., M. G. Morris, G. B. Davis, and F. D. Davis, "User acceptance of information technology: Toward a unified view", *MIS Quarterly*, Vol.27, No.3, 2003, pp. 425-478.

[61] Voiskounsky, A. E. and O. V. Smyslova, "Flow-based model of computer hackers' motivation", *Cyber Psychology and Behavior*, Vol.6, No.2, 2003, pp. 171-180.

[62] Wetzels, M., G. Odekerken-Schröder, and C. Van Oppen, "Using PLS path modeling for assessing hierarchical construct models: Guidelines and empirical illustration", *MIS Quarterly*, Vol.33, No.1, 2009, pp. 177-195.

[63] Young, R., L. Zhang, and V. R. Prybutok, "Hacking into the minds of hackers", *Information Systems Management*, Vol.24, No.4, 2007, pp. 281-287.

[64] Zhao, M., J. Grossklags, and K. Chen, "An exploratory study of white hat behaviors in a web vulnerability disclosure program", In *Proceedings of the 2014 ACM Workshop on Security Information Workers*, ACM, 2014, pp. 51-58.

Information Systems Review
Volume 19 Number 3
September 2017

How Vulnerability Research Motives Influence the Intention to Use the Vulnerability Market?

Hyeong-Yeol Kim* · Tae-Sung Kim**

Abstract

Vulnerability information, which can cause serious damage to information assets, has become a valuable commodity, thereby leading to the creation of a vulnerability market. Vulnerability information is traded on the vulnerability market from several hundred dollars to hundreds of thousands of dollars depending on its severity and importance, and the types and scope of the vulnerability markets are varying. Based on previous studies on vulnerability markets and hackers, this study empirically analyzed the effects of the security researcher's vulnerability research motivation on his/her vulnerability market use intention. The results are discussed as follows. First, vulnerability research self-efficacy had a significant effect on flow and on white and black market use intention but not on perceived benefit. Second, flow had a significant effect on perceived benefit and on black market use intention but had no effect on white market use intention. Third, perceived profit had a significant effect on white and black market use intention. Fourth, vulnerability research self-efficacy had a significant effect on perceived benefit through flow. Fifth, flow had a significant effect on white and black market use intention through perceived profit. These findings can be used to predict the behavior of security researchers who have experience in exploiting vulnerabilities.

Keywords: ***Security Researcher, Vulnerability Market, Vulnerability Research Self-Efficacy, Flow, Perceived Benefit, Vulnerability Market Use Intention***

* A3 Security Co., Ltd.
** Corresponding Author, Department of Management Information Systems, Chungbuk National University

◐ 저 자 소 개 ◑

김 형 열 (khy786@hanmail.net)

한남대학교 경찰행정학과에서 행정학 학사를 취득한 후, 충북대학교 정보보호경영학과에서 경영학 석사를 취득하였다. 현재 주식회사 에이쓰리시큐리티에서 재직하고 있다. 한국경영정보학회, 한국정보보호학회, 한국정보기술응용학회, International Conference on Digital Policy & Management 등 국내외 정보보호, 경영정보 관련 학술지 및 학술대회에 논문을 발표하였다. 주요 관심분야는 취약점마켓, 정보보호컨설팅 및 정보보호서비스이다.

김 태 성 (kimts@cbnu.ac.kr)

한국과학기술원 산업경영학과에서 박사를 취득하고 한국전자통신연구원 정보통신기술경영연구소에서 근무한 후, 현재 충북대학교 경영정보학과에서 정교수로 재직하고 있으며 대학원 정보보호경영전공 주임교수와 보안경제연구소장을 맡고 있다. University of North Carolina at Charlotte과 Arizona State University에서 Visiting Professor와 Visiting Scholar로 각각 근무하였다. OR Letters, European Journal of Operation Research, Journal of the Operational Research Society 등 국내외 경영과학, 정보통신, 관련 학술지 및 학술대회에 논문을 발표하였으며, 주요 관심분야는 정보통신과 정보보호 분야의 경영 및 정책 의사결정이다.

논문접수일 : 2017년 07월 18일 **게재확정일 : 2017년 09월 27일**
1차 수정일 : 2017년 09월 13일