Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.1, Feb. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.1.207

정보보안이 스마트폰 선택에 미치는 영향에 관한 연구

안 종 창,† 이 승 원, 이 욱,‡ 조 성 필
한양대학교

A study on the influence of information security in selecting smart-phone

Jong-chang Ahn,† Seung-won Lee, Ook Lee,‡ Sung-phil Cho
Hanyang University

요 약

최근 스마트폰 스파이웨어는 PC의 여러 가지 유형의 바이러스 요소들을 닮아가고 있으며, 점점 심각해지고 있는 추세이다. 또한 스마트폰 스파이웨어의 성장속도에 비해 스마트폰의 보안과 관련된 측면들은 매우 취약한 상태이지만 사용자들은 그러한 위험 요소들을 심각하게 인지하지 못하고 있는 실정이다. 이에 본 연구는 개인적 성향과 스파이웨어에 대한 인식을 바탕으로 정보보안이 스마트폰 선택에 미치는 영향을 살펴본다. 연구 모델의 주요 변수는 독립 변수로 개인별 위험성 감수정도와 스마트폰 스파이웨어 위험성을 선정하고, 종속 변수로 스마트폰 구매 의향을 설정하였다. 현재 스마트폰을 사용하고 있는 사용자를 대상으로 설문조사를 통해 얻은 200부의 유효한 자료를 SPSS 21 통계 프로그램을 이용하여 검증하였다. 연구결과에 의하면 개인별 위험성 감수정도에 따라 스마트폰 스파이웨어의 위험성을 인지하는 것과, 스마트폰 스파이웨어의 위험성을 인지할수록 스마트폰 구매의향에 영향을 미치는 것으로 나타났다. 즉, 스마트폰을 선택할 때 정보보안의 영향을 파악할 수 있었다.

ABSTRACT

Recently, smartphone spyware resembles various types of virus components in PCs and has trends getting more and more severe. Users do not perceive the risk factors severely even if smartphone security is very vulnerable in spite of the smartphone spyware growth. Thus, this study observes the influence of information security in selecting smartphone based on the personal inclinations and spyware perceptions. The main variables of study model are such as the degree of personal risk-accepting and the risk of smartphone spyware as independent variables and smartphone purchasing intention as a dependent variable. The model is tested using SPSS 21 packages on the effective 200 samples gathered through questionnaire survey on the present smartphone users. As a result, the two main hypotheses which are "the degree of personal risk-accepting will influence on the perceiving risk of smartphone spyware" and "the perceiving risk of smartphone spyware will influence on smartphone purchasing intention" were significant statistically. Therefore, we could find out information security's influence on the selecting smartphone.

Keywords: risk-accepting, purchasing intention, smartphone security, spyware

I. 서 론

스마트폰은 일반폰 보다 진일보한 성능을 지닌 PC와 유사한 기능의 모바일 단말을 의미한다. 최근 아이폰 및 안드로이드폰의 성장을 바탕으로 세계적으로 모바일 시장에서 시장 점유율이 급격히 증가하고 있는

접수일(2013년 12월 17일), 수정일(2014년 1월23일), 게재확정일(2014년 1월 23일)
† 주저자, ajchang@hanyang.ac.kr
‡ 교신저자, ooklee@hanyang.ac.kr (Corresponding author)

추세이며[1], 국내의 경우 스마트폰은 2010년 초부터 급격히 성장하여 2011년부터 신규 단말기의 60% 이상이 스마트폰으로 판매되고 있다[2]. 스마트폰은 PC와 유사한 수준의 강력한 성능을 바탕으로 사용자에게 다양한 서비스를 제공할 수 있다. 기본적으로 사용자는 스마트폰을 사용하여 일반 휴대폰과 마찬가지로 음성통화, 문자메시지, 멀티미디어 메시지(MMS) 등의 기능을 사용할 수 있으며, 그 외 스마트폰의 다양한 응용프로그램을 바탕으로 여러 가지 서비스를 부가적으로 이용할 수 있다[1].

이러한 스마트폰은 누구나, 언제나, 어디서나 가능한 유비쿼터스 서비스 환경에 대한 편의성 측면에서 사용자에게 더없이 좋은 일이지만 한편으로는 나의 모든 행동과 일상이 관찰, 기록, 저장됨을 의미하며, 이것은 현대인의 개인주의적인 성향과는 반대의 성격으로 풀이된다[3]. 스마트폰은 PMP, MP3 Player, 전자사전, 지도 등으로 확장된 다양한 모바일 기기의 융합 형태로 발전하고 있으나, 이런 현상은 그만큼 다양한 정보가 스마트폰에 집중된다는 것을 의미한다. 스마트폰은 휴대용 기기로서 분실의 우려가 높고, 통화, 문자메시지, 무선네트워크 접속 등의 서비스는 과금과 직접적인 연관이 있기 때문에 스마트폰의 취약성은 정보의 손실뿐만 아니라 금전적 피해도 야기할 수 있는 실정이다[1]. 또한, 최근 스마트폰 이용 확산에 따라 시간과 장소에 구애 받지 않고 무선 인터넷을 이용한 스마트폰을 활용하면서 기존 PC환경에서의 보안위협이 스마트폰 환경에서도 나타나고 있으나, 다양한 유형의 공격 심각성을 사용자들이 정확히 인지하지 못하고 있는 상황이다. 또한 스마트폰의 총체적인 보안위협과 그에 대한 대응기술에 대한 정의가 명확하지 않은 실정이다. 여러 바이러스의 성장속도에 비해 스마트폰의 보안과 관련된 측면들은 취약한 점에 관한 우려의 목소리가 높아지면서, 스마트폰 보안이 최근 중요한 이슈로 부각되고 있다.

본 논문의 주요 목적은 개인별 위험성 감수정도가 스마트폰 스파이웨어 위험성을 인지하는지, 개인별 위험성 감수 정도가 이 스마트폰 구매의향에 영향을 미치는지, 스마트폰 스파이웨어의 위험성 인지가 스마트폰 구매의향에 영향을 미치는지 여부다. 부가적으로 스마트폰 종류에 따라서 위험성을 감수하는 정도에 차이가 있는지, 스파이웨어 위험성을 지각하는데 차이가 있는지, 스마트폰 구매 의향에 차이가 있는지를 살펴본다. 또한 성별에 따라 위험성을 감수하는 정도에 차이가 있는지, 스마트폰 스파이웨어의 위험성을 지각하는데 차이가 있는지, 스마트폰 구매 의향에 차이가 있는지를 살펴본다. 나이에 따라 개인별 위험성 감수 정도, 스마트폰 스파이웨어 위험성을 지각하는데 차이가 있는지, 스마트폰 구매의향에 차이가 있는지에 대해 또한 살펴본다.

본 논문은 먼저 연구 배경과 목적을 제시하고, 다음으로 이론적 배경으로 스마트폰 보안위협 요소와 악성코드 및 위협에 대해 살펴본다. 그 다음으로 실증분석을 하며 마지막으로 결론과 한계점을 제시하는 것으로 구성되어 있다.

II. 이론적 배경

2.1 스마트폰 보안위협 요소

최근 스마트폰 이용 확산에 따라 시간과 장소에 구애 받지 않고 무선 인터넷을 활용하면서 기존 인터넷 사이트의 환경도 스마트폰 환경 변화에 맞춰 변화되고 있다. PC환경에서 제공하는 인터넷 서비스가 스마트폰 환경으로 전환되면서 PC환경의 보안 위협이 스마트폰 환경에서도 나타나고 있다. PC를 대상으로 나타나는 다양한 유형의 공격은 백신, 방화벽 및 침입탐지 기술로 대응을 하고 있지만 이에 비해 스마트폰은 다양한 무선 접속환경의 개방성, 휴대성, 저성능 등으로 기존 PC환경의 보안 위협과 더불어 새로운 보안 위협에 노출되어 있다. 이러한 스마트폰의 사용 환경에 대한 보안 위협은 개방성, 휴대성, 저성능과 관련하여 살펴볼 수 있다.

스마트폰이 일반 휴대폰과 구분되는 가장 큰 특성은 개방성이다. 즉, 일반 휴대폰과 다르게 무선인터넷 및 외부 인터페이스를 개방하여 제공하고 있고, 애플리케이션 개발 시 시스템 자원의 사용을 위해 서비스 개발키트(SDK)를 이용하여 애플리케이션 프로그래밍 인터페이스(API)를 제공하고 있다. 스마트폰의 다양한 외부 인터페이스는 사용자에게 편리하고 다양한 네트워크 서비스를 지원하며 내부 API 인터페이스 제공은 개발자가 편리하게 개발할 수 있는 환경을 제공한다. 하지만 이를 보안적인 측면에서 해석하면, 다양한 외부 인터페이스 제공은 악성코드 전파 경로가 다각화 되어 악성코드가 쉽게 퍼지는 결과를 가져왔다. 내부 인터페이스는 악의적인 개발자가 모바일 애플리케이션에 악성코드를 쉽게 은닉하여 제작할 수 있도록 만드는 취약점을 가져왔다[4].

스마트폰의 휴대 편의성으로 인해 발생하는 분실,

도난율이 매우 높으며, 스마트폰 분실, 도난에 따른 직접적인 경제적 피해와 더불어 스마트폰에 저장된 개인 정보 및 이메일, 전자결재, 기밀정보 등 개인 사생활과 업무 관련 중요 정보의 유출은 심각한 사회문제를 야기할 수도 있다[4].

스마트폰은 PC에 비해 저 전력, 저성능 기기이다. 따라서 PC환경에서 제공하는 보안 소프트웨어를 스마트폰에 적용하기에는 무리가 있다. PC환경에서는 다양한 보안 위협에 대응하기 위해서 지속적인 모니터링을 통해 악성코드를 탐지해야 하지만, 스마트폰은 전력 및 성능적인 제약으로 인해 백신을 비롯한 보안 소프트웨어의 적용에 어려움이 있다[5].

2.2 스마트폰 악성코드

스마트폰 악성코드는 스마트폰에서 동작하면서 시스템을 파괴하거나 저장된 개인정보 등을 유출하는 악의적 활동을 수행하는 코드이다. 스마트폰 악성코드는 스마트폰의 성장과 더불어 규모면에서 빠르게 증가하고 있고 위협요인도 다양화되고 있다. 스마트폰 악성코드가 증가하는 원인은 악의적인 목적을 가진 악성코드의 제작 및 유통이 가능한 개방형 스마트폰의 증가와 함께 블루투스, Wi-Fi와 USB 등 외부 접속의 다양화가 원인이라고 할 수 있다. 스마트폰 악성코드는 초기에 단순히 전파를 목적으로 하거나 단말의 기능적 동작을 마비시키는 형태에서, 개인정보의 유출 및 금전적 이득을 목적으로 하는 형태로 변화하고 있다[6].

지금까지 존재한 스마트폰 악성코드를 주요 활동별 특성을 반영하여 분류하면 5가지 형태로 구분할 수 있다[5].

먼저, 단말 장애 유발형 악성코드이다. 스마트폰의 사용을 불가능하게 만들거나 장애를 유발하는 공격 유형이다. 2004년에 발견된 Skulls가 단말의 기능을 마비시키는 단말 기능 마비형 악성코드 유형이다. 이 악성코드는 모든 메뉴 아이콘을 해골로 변경시키고 통화 이외의 부가기능을 사용할 수 없게 만든다. 2005년에 발견된 Locknut 악성코드는 스마트폰의 일부 키 버튼을 고장 내는 특성을 가지고 있다. 이외에도 전화의 송수신 기능을 마비시키는 Gavno가 등장하였다[6].

두 번째는 배터리 소모형 악성코드이다. 스마트폰의 전력을 지속적으로 소모시켜 배터리를 고갈시키는 공격 유형이다. 2004년에 블루투스를 통해 전파되는 최초의 모바일 악성코드인 Cabir가 대표적이다. Cabir는 스마트폰의 침해를 유발하지 않는 대신 지속적으로 인근 스마트폰의 블루투스를 스캐닝하고, 블루투스를 통해 악성코드를 전파하는 특징을 가지고 있다. 감염된 스마트폰은 지속적인 스캐닝을 통해 배터리의 고갈 피해를 입게 된다[5].

세 번째는 과금 유발형 악성코드이다. 스마트폰의 메세징 서비스나 전화 시도를 지속적으로 시도하여 과금을 발생시키는 공격 유형이다. 2006년 러시아에서 제작된 J2me 플랫폼용 RedBrowser가 대표적인 사례로써 감염된 스마트폰은 사용자도 모르게 불특정 다수에게 SMS를 전송함으로써 사용자에게 금전적 피해를 입히는 악성코드이다. 또한 중국에서 2008년에 발견된 Kiazha 악성코드는 감염된 단말 화면에 사용자에게 돈을 요구하는 경고 메시지와 함께 단말 내에 저장된 문자메세지를 삭제하는 악성코드가 등장하였다. 2010년 4월, 국내에서 최초로 발생한 스마트폰 악성코드인 WinCE/TerDial은 게임 내에 숨겨진 형태로 존재하며 국제전화를 송신하여 사용자에게 피해를 입히는 시도를 했다[4].

네 번째는 정보유출형 악성코드이다. 감염된 스마트폰의 정보나 사용자 정보를 외부로 유출시키는 공격 유형이다. 2008년 발견된 Infojack이 대표적인 예이다. 이 악성코드는 합법적인 애플리케이션이 스마트폰에 다운로드 될 때 .cab 설치파일과 함께 포함되어 설치되고, 설치된 후 특정 웹 서버에 접속하여 Infojack의 나머지 부분을 다운로드하여 재설치 한다. 설치가 완료되면 스마트폰의 보안 설정을 변경하고 스마트폰의 시리얼 번호, OS, 설치된 애플리케이션 등 스마트폰의 정보를 외부로 전송하여 2차 공격을 용이하게 한다. 사용자의 정보를 외부로 유출시키는 악성코드로는 Flexispy, PBStealer가 있다. Flexispy는 스파이웨어 형태의 상용 악성코드로써 스마트폰의 전화기록, 문자메세지 내용을 특정 웹서버로 전송하는 기능을 가지고 있다[5].

마지막 유형은 크로스 플랫폼형 악성코드이다. 스마트폰을 통해 PC를 감염시키는 공격 유형이다. 2005년에 발생된 Cardtrap.A가 최초의 이런 악성코드로써 스마트폰의 메모리 카드에 윈도 웜을 복사하여, 감염된 스마트폰 메모리 카드를 PC에 장착했을 때 autorun을 통해 PC를 자동으로 감염시켜 데이터를 삭제하거나 성능을 저하시킨다. 스마트폰 기기간의 확산이 아닌 스마트폰 기기에서 PC를 감염시킨다는 점에서 새로운 형태의 공격유형이라 볼 수 있다[6].

2.3 위협

위협 분류 체계는 알려진 공격 방법뿐 아니라 예상도 할 수 있어야 하지만, 모바일 공격에 대한 탐지 및 방지 시스템은 초기 단계에 있다. 따라서 모바일 네트워크에 대한 보안 연구는 라우팅 문제에 주로 초점을 맞추는 것과 프로토콜 보안을 계속 최신 버전으로 유지시키는 데에 있다. 공격자가 프로토콜 스택을 개발하는 법을 고안하는 것처럼 모바일 위협의 위험요소의 분석을 유의해서 스마트폰 보안을 강화해 악의적인 공격자의 공격을 방어해야 한다[7]. 모바일 전화기 자체에 대한 위협에 국한해 보면 위협은 i) 정보 절도, ii) 요청되지 않은 정보, iii) 서비스 절도, iv) 서비스 거부로 분류할 수 있다. 해커들은 일시적 정보와 정적 정보를 획득하기 위해 모바일 장치를 공격하는 정보 절도를 한다. 요청되지 않은 정보로는 스팸 SMS 메시지와 Bluejacking(블루투스 장치 이름을 설정해서 메시지를 광고하고 다른 사용자들이 그것을 발견토록 함)이 있다. 어떤 맬웨어는 피해자(victim)의 전화기 자원을 이용하려고 하는 서비스 절도이며 Mosquitos 바이러스가 예이다. 마지막으로, 모바일 전화기에 대한 서비스 거부의 두 가지 형태는 장치를 넘치도록(flooding) 하는 시도와 전력을 소진하려는 시도가 있다[7].

III. 연구의 방법

3.1 연구 모형

본 연구는 어떠한 요소들에 의해 스마트폰 선택이 영향을 받는지 알아보고자 한다. 연구 모형은 앞의 이론적 배경에서 논의한 사항을 바탕으로 개인별 위험성 감수 정도, 스마트폰 스파이웨어 위험성 인지, 스마트폰 구매의향에 영향력을 변수로 추출하여 정보보안의 스마트폰 선택에 대한 영향 정도를 알아보고자 한다. 구체적으로 설정된 가설은 다음과 같다.

가설 1. 개인별 위험성 감수 정도가 스마트폰 스파이웨어 위험성을 인지할 것이다.
가설 2. 개인별 위험성 감수 정도가 스마트폰 구매의향에 영향을 미칠 것이다.
가설 3. 스마트폰 스파이웨어의 위험성 인지가 스마트폰 구매의향에 부(-)의 영향을 미칠 것이다.
가설 4. 스마트폰 종류에 따라 위험성을 감수하는 정도에는 차이가 있을 것이다.
가설 5. 스마트폰 종류에 따라 스파이웨어 위험성을 지각하는 데는 차이가 있을 것이다.
가설 6. 스마트폰 종류에 따라 스마트폰 구매 의향에 차이가 있을 것이다.
가설 7. 성별에 따라 위험성을 감수하는 정도에는 차이가 있을 것이다.
가설 8. 성별에 따라 스마트폰 스파이웨어의 위험성을 지각하는 데는 차이가 있을 것이다.
가설 9. 성별에 따라 스마트폰 구매 의향에는 차이가 있을 것이다.
가설 10. 개인별 위험성 감수 정도에는 나이가 영향이 있을 것이다.
가설 11. 스마트폰 스파이웨어 위험성을 인지하는 것에 나이가 영향이 있을 것이다.
가설 12. 스마트폰 구매의향에는 나이가 부(-)의 영향을 미칠 것이다.

연구 모형은 결국 사용자가 스마트폰을 구매하고 사용하는 데 있어서 정보보안이 얼마나 영향을 끼치는지, 심각성을 잘 인지한다면 스마트폰을 다음 기회에도 구매하는데 영향을 주는가에 대해 주로 알아보고자 한다. 이 연구의 연구모형은 Fig.1.과 같이 요약할 수 있다.

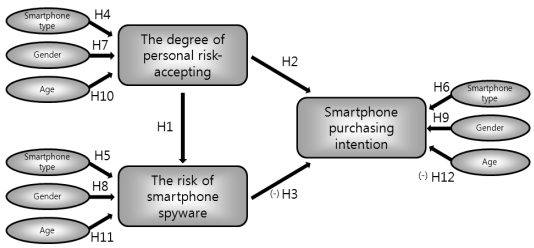


Fig.1. Research model: the influence on smartphone selection by information security

3.2 표본 구성과 설문의 구성

본 연구는 정보보안이 스마트폰 선택에 미치는 영향을 고찰하기 위해 실제 스마트폰을 사용해 본 사람들을 실험대상자로 하여 온라인 설문조사를 수행하였다. 설문조사기간은 2013년 5월 1일부터 2013년 7월 3일이며, 조사결과 처음부터 끝까지 모든 항목에 대해 성실히 응답한 총 200명 응답자들의 데이터를

통계적 분석 자료로 사용하였다.

본 설문은 총 14문항으로 일반현황에 대한 질문 3문항, 개인별 위험성 감수 정도에 대한 질문 6문항, 스마트폰 스파이웨어 위험성에 대한 질문 2문항, 그리고 마지막으로 스마트폰 구매의향에 대한 질문 2문항, 기타 1문항으로 구성되어 있다. 일반 현황과 5점 등간척도에 예외 대답을 더한 질문 1개를 제외한 나머지 질문은 리커트 5점 등간척도(1=전혀 아니다, 2=아니다, 3=보통이다, 4=그렇다, 5=아주 그렇다)를 이용하였다.

설문지의 결과 분석을 위하여 통계패키지 SPSS 21을 사용하였으며, 신뢰성 분석, 단순회귀분석, 독립표본 t-검정을 통해 설정된 가설을 검증했다.

IV. 연구결과 분석

4.1 표본의 특성

설문에 응답한 표본의 구성은 다음과 같다. 설문 응답자의 성별은 최종적으로 이용된 200명의 데이터 중 남자가 63명(31.5%)으로 여자 137명(68.5%)보다 다소 적게 나타났다. 설문 응답자의 연령대는 스마트폰을 많이 사용하는 20대(62%)와 30대(24.5%)가 다수를 차지하고 있다. 설문응답자의 직업은 사무/기술직(28.5%)과 대학생(28.5%), 자유/전문직(10.5%)이 다수를 차지하고 있다. 설문응답자의 거주 지역은 서울(26.5%)과 경기(23.5%)가 다수 분포되어 있는 것으로 나타났다.

4.2 타당성 및 신뢰성 분석

다 항목으로 측정된 이론변수는 이를 구성하는 측정항목들이 해당 이론변수를 적절하게 반영하였는가와 관련하여 신뢰도를 평가할 필요가 있다[8]. 본 연구에서는 신뢰성을 측정하기 위해서 각 문항에 대한 신뢰성 검증으로 많이 사용되는 크론바 알파 계수를 사용하였다. 개인별 위험성 감수정도(0.677), 스마트폰 스파이웨어 위험성(0.682)을 설명해주는 가설설정 변수들 간의 Cronbach α 계수는 0.6 이상 기준을 충족하여 신뢰성 있는 측정항목으로 측정되었다[9]. 하지만 스마트폰 구매의향(종속변수)에 대한 측정은 임계치인 0.6에 미치지 못해서 "스마트폰을 새로 구입한다면 이 위험성을 고려해서 구매할 것이다"는 항목을 추가하여 분석을 진행하였다. 타당성과 신뢰성에 대해 기본적으로 Van de Van (1980)의 방식을 활용했으며, 측정도구의 타당성은 요인 분석을 이용하여 검증하였으며 주성분 분석과 요인 적재량(공통성)을 기준으로 부합하는 측정 항목으로 구성되었다.

4.3 가설 검증

가설 검증을 위하여 모든 가설을 회귀분석이나 독립표본 t-검정을 통해 분석을 실행하였다[10].

개인별 위험성 감수 정도에 따라 스마트폰 스파이웨어 위험성을 인지 할 것이다(가설 1)에 대한 분산분석에 의하면, F값은 13.671로 나타났고(유의확률은 0.000) 회귀선의 모델이 적합하다는 것을 알려준다. 또한 계수를 보면, 기울기에 대한 추정치는 0.460, 기울기 표준오차는 0.124로 나타나고 있다. t값은 3.697로서 ± 1.96보다 크고, 유의확률(p)은 0.000로서 $p<.01$이므로 1% 유의 수준에서 **가설 1을 채택**할 수 있다.

개인별 위험성 감수 정도에 따라 스마트폰의 구매의향이 바뀔 것이다(가설 2)에 대한 분산분석에 의하면, F값은 0.623으로(유의확률은 0.431) 회귀선의 모델이 부적합하다는 것을 알려준다. 또한 계수를 보면, 기울기에 대한 추정치는 -0.092, 기울기 표준오차는 0.116으로 나타나고 있다. t값은 -.789로서 ± 1.96보다 작고, 유의확률(p)은 0.431로서 $p>.05$이므로 5% 유의수준에서 가설 2를 채택할 수 없다.

스마트폰 스파이웨어 위험성을 인지함에 따라 스마트폰 구매의향에 부(-)의 영향을 미칠 것이다(가설 3)에 대한 분산분석을 보면, F값은 8.968로 나타나고(유의확률은 0.003) 회귀선의 모델이 적합하다는 것을 알려준다. 또한 계수를 보면, 기울기에 대한 추정치는 -0.189, 기울기 표준오차는 0.063으로 나타나고 있다. t값은 -2.995로서 ± 1.96보다 크고, 유의확률(p)은 0.003으로서 $p<.01$이므로 1% 유의 수준에서 **가설 3을 채택**할 수 있다.

스마트폰 종류에 따라 위험성을 감수하는 정도에는 차이가 있을 것이다(가설 4)의 평균 차이는 F값의 유의확률이 0.587로 0.05를 넘으므로 등분산이 가정되었지만, t값이 1.659로, $p>.05$이므로($p=0.099$) 5% 유의수준에서 가설 4를 채택할 수 없다.

스마트폰 종류에 따라 스파이웨어 위험성을 지각하는 데는 차이가 있을 것이다(가설 5)의 평균 차이는 F값의 유의확률이 0.142로 0.01을 넘으므로 등분산이 가정되었고, t값이 3.575로, 통계적 유의수준인

0.01보다 작으므로(p=0.000) 1% 유의수준에서 **가설 5를 채택**할 수 있다.

스마트폰 종류에 따라 스마트폰 구매 의향에 차이가 있을 것이다(가설 6)의 평균 차이는 F값의 유의확률이 0.842로 0.05를 넘으므로 등분산이 가정되었고, t값이 -3.325로, 통계적 유의수준인 0.01보다 작으므로(p=0.001) 1% 유의수준에서 **가설 6을 채택**할 수 있다.

성별에 따라 위험성을 감수하는 정도에는 차이가 있을 것이다(가설 7)의 평균 차이는 F값의 유의확률이 0.604로 0.01을 넘으므로 등분산이 가정되었고, t값이 3.133으로, 통계적 유의수준인 0.01보다 작으므로(p=0.002) 1% 유의수준에서 **가설 7을 채택**할 수 있다.

성별에 따라 스마트폰 스파이웨어의 위험성을 지각하는 데는 차이가 있을 것이다(가설 8)의 평균 차이는 F값의 유의확률이 0.172로 0.05를 넘으므로 등분산이 가정되었고, t값이 2.520으로, 통계적 유의수준인 0.05보다 작으므로(p=0.013) 5% 유의수준에서 **가설 8을 채택**할 수 있다.

성별에 따라 스마트폰 구매 의향에는 차이가 있을 것이다(가설 9)의 평균 차이는 F값의 유의확률이 .492로 0.05를 넘으므로 등분산이 가정되었지만, t값이 -1.119으로, 통계적 유의수준인 0.05보다 크므로(p=0.264) 5% 유의수준에서 가설 9를 채택할 수 없다.

개인별 위험성 감수 정도에는 나이가 영향이 있을 것이다(가설 10)의 분석 계수를 보면, 기울기에 대한 추정치는 -.001, 기울기 표준오차는 0.007로 나타나고 있다. t값은 -.074로서 ± 1.96보다 작고, 유의확률(p)은 0.941로서 p〉.05이므로 5% 유의 수준에서 가설 10을 채택할 수 없다.

스마트폰 스파이웨어 위험성을 인지하는 것에는 나이가 영향이 있을 것이다(가설 11)의 분석 계수를 보면, 기울기에 대한 추정치는 0.017, 기울기 표준오차는 0.012로 나타나고 있다. t값은 1.393으로서 ± 1.96보다 작고, 유의확률(p)은 0.165로서 p〉.05이므로 5% 유의 수준에서 가설 11을 채택할 수 없다.

스마트폰 구매의향에는 나이가 부(-)의 영향을 미칠 것이다(가설 12)의 분석 계수를 보면, 기울기에 대한 추정치는 -0.029, 기울기 표준오차는 0.010으로 나타나고 있다. t값은 -2.760으로서 ± 1.96보다 크고, 유의확률(p)은 0.006로서 p〈.01이므로 1% 유의수준에서 **가설 12를 채택**할 수 있다.

4.4 가설 검증결과

이상의 가설들에 대한 연구결과(채택된 가설 기준)는 다음 Fig.2.와 같이 요약할 수 있다.

본 연구에 의해 드러난 정보보안이 스마트폰 선택에 미치는 영향의 방향을 요약하면 다음과 같다. 개인별 위험성 감수정도에 따라 스마트폰 스파이웨어 위험성을 인지하는데 영향을 미치고 있으며(H1), 스마트폰 스파이웨어 위험성을 인지함에 따라 스마트폰 구매의향에 영향을 미치고 있다(H3). 또한, 스마트폰 종류가 무엇이든 개인이 위험성을 감수하는 정도에는 차이가 없으며, 스마트폰 종류에 따라 스파이웨어 위험성을 지각하는 것(H5)과 스마트폰을 구매하는 것(H6)에 영향을 미치게 된다. 그리고 성별에 따라 개인별 위험성 감수정도(H7)와 스마트폰 스파이웨어의 위험성을 인지하는 것(H8)에 상관이 있지만, 성별에 따른 스마트폰을 구매하는 의향에는 차이가 없었다. 마지막으로, 개인별 위험성 감수정도와 스마트폰의 스파이웨어 위험성을 인지하는 것에 나이는 유의한 상관이 없었다. 하지만 나이가 많을수록 스마트폰 구매의사가 더욱 망설여지고 신경 쓰이게 되는 부의 영향을 준다는(H12) 것이 확인되었다.

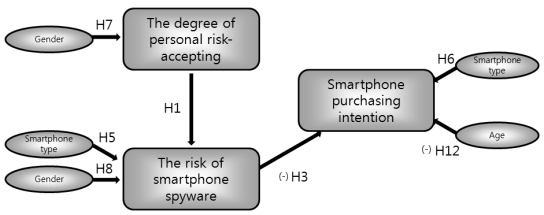


Fig.2. Research results: the influence on smartphone selection by information security

V. 결 론

5.1 연구결과 및 시사점

스마트폰은 PC와 유사한 수준의 강력한 성능을 바탕으로 사용자에게 다양한 서비스를 제공함으로써 최근 PC 산업이 발전해온 속도보다 훨씬 빠르게 앞으로도 기술의 진보를 계속할 것으로 보인다. 이에 따라 본 연구에서는 급격하게 성장하고 있는 스마트폰 시장에 따라 국내 스마트폰 악성코드의 등장과 이로 인한 피해가 예상되는 현 시점에서, 그 심각성을 알리고자 하였다. 본 연구는 기존에 연구가 미비하였던 스마트

폰 관련 위험성 인지와 스파이웨어에 대한 위험성 인지가 스마트폰 선택에 영향을 미치는 것에 대해 체계적 가설설정과 이를 바탕으로 통계적 분석을 하였다는 점에서 스마트폰 정보보안연구에 이론적 기여를 하였다. 이를 바탕으로 도출된 유의한 사항들은 스마트폰의 정보보안에 대한 고려할 요소로 여러 가지 시사점을 가진다.

또한, 본 연구결과는 실무적으로 정보보안에 대한 사용자의 인식을 반영하여 스마트폰의 제품 설계와 서비스를 제공하는데 참조할 수 있다. 이론적으로 이 분야에 대한 행태 연구가 다소 부족하여 탐색적 성격이 있지만, 본 연구결과를 바탕으로 좀 더 정교한 스마트폰 선택(구매) 의향에 대한 기초가 될 수 있다는 점에서 연구의 시사점을 찾을 수 있다.

5.2 연구의 한계점 및 향후 과제

본 연구는 샘플의 고른 분포를 위해 온라인 서베이를 통해 데이터가 수집되었다. 다소 탐색적 성격의 연구로 인해 변수들에 대한 측정항목들이 좀 더 정교하게 보완되고 좀 더 구체적인 이론 바탕 하에 구성될 필요성이 있으며 구조방정식 모형(SEM)에 의한 분석이 추가될 수 있다. 스마트폰 종류에서 안드로이드와 아이폰 계열 두 부류만을 대상으로 했지만, 향후 연구에서는 좀 더 다양한 종류의 스마트폰에 대한 분석이 이루어질 필요성이 있다. 또한 본 연구는 국내 스마트폰 사용자들에 대한 행태분석으로, 다른 국가에서의 사용자들에 대한 분석이 추가될 여지가 있다. 이를 통해 비교 분석이 이루어진다면, 좀 더 일반적인 이론 틀로의 진전이 가능하리라 본다.

References

[1] Woongyeol Cheon, Jiyeon Kim, Youngsook Lee, Dongho Won, "Samrtphone security threats and responding technology analysis," *Journal of The Korea Society of Computer and Information*, 16(2), pp. 153-163, Feb. 2011.

[2] Heyonook Kim, "Smartphone technology development and security technology trends," *Telecommunications Review*, 21(2), pp. 219-241, Mar. 2011.

[3] Hyeonah Park, Jaetag Choi, Jongin Lim, Donghun Lee, "Analytical study on the individual information threats in mobile environments," *Review of KIISC*, 17(4), pp. 56-73, Aug. 2007.

[4] Seunghyeon Seo, Kilsoo Cheon, "Samrtphone security threats and responding technology," *TTA Journal*, 132, pp. 44-48, Nov./Dec. 2010.

[5] Dongho Kang, Jinhee Han, Youn- keyong Lee, Yourngsub Cho, Seong-wan Han, Jeongyeo Kim, Heonsook Cho, "Samrtphone security threats and corresponding technology," *Electronics and Telecommunications Trends*, 25(23), pp. 72-80, Jun. 2010.

[6] Kiyoung Kim, Dongho Kang, "Smartphone security technology in open mobile environments," *Review of KIISC*, 19(5), pp. 21-28, Oct. 2009.

[7] Dong-Her Shih, Binshan Lin, Hsiu-Sen Chiang, and Ming-Hung Shih, "Security aspects of mobile phone virus: a critical survey," Industrial Management & Data Systems, vol. 108, no. 4. pp. 478-494, 2008.

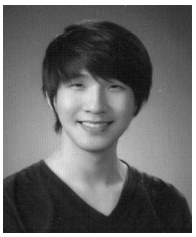
[8] Gilbert A. Churchill, and Jr.,J. Paul Peter, "Research design effects on the reliability of rating scales: a meta analysis," Journal of Marketing Research, vol. 11, pp. 360-375, Nov. 1984.

[9] A. H. Van de Van, and D. L. Ferry, Measuring and assessing organization, Wiley Inter science, New York, 1980.

[10] Mincheol Shin, The basic managerial and economic statistics, Changmin publisher, Seoul, Mar. 2010.

〈저자소개〉

안 종 창 (Jong-chang Ahn) 정회원
1994년 2월: 고려대학교 경제학과 졸업
2002년 8월: 세종대학교 인터넷소프트웨어학과 석사
2007년 8월: 한양대학교 정보기술경영학과 박사
2010년 9월~현재: 한양대학교 정보시스템학과 조교수
〈관심분야〉 정보보호, 지식경영, 정보시스템 감사



이 승 원 (Seung-won Lee) 정회원
2011년 2월: 극동대학교 컴퓨터시스템표준학과 졸업
2014년 2월: 한양대학교 정보시스템학과 석사
〈관심분야〉 정보보호, 모바일 폰

이 욱 (Ook Lee) 정회원
1987년 2월: 서울대학교 계산통계학과 졸업
1989년 6월: Northwestern대학교 전산학과 석사
1997년 1월: Claremont대학교 경영정보학과 박사
2002년 3월~현재: 한양대학교 정보시스템학과 교수
〈관심분야〉 정보보호, IT 행태/철학/응용

조 성 필 (Sung-phil Cho) 정회원
2008년 2월: 한양대학교 정보기술경영학과 졸업
2011년 1월: Claremont대학교 경영정보학과 석사
2014년 2월: 한양대학교 정보기술경영학과 박사
〈관심분야〉 IT 거버넌스, 정보보호, 전자정부