Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.1, Feb. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.1.285

Facebook의 Usable Security에 관한 연구*

김 청 한,† 박 민 수, 김 승 주‡
고려대학교 정보보호대학원

Study on Usable Security of Facebook*

Chung-han Kim,† Min-su Park, Seung-joo Kim‡
Center for Information Security Technologies(CIST), Korea University

요 약

최근 스마트 폰과 테플릿 PC를 통한 Facebook의 사용이 보편화되고 있는 반면, Facebook에서 공개되는 개인 정보를 이용한 사회 공학적 공격과 악성코드가 포함된 댓글 및 게시물이 배포되는 등의 보안 위협 또한 증가하고 있다. 이러한 문제를 해결하기 위해 Facebook에서는 다양한 보안 기능을 제공하고 있는데, 보안 기능에 사용자의 편의성을 결합시킨 Usable Security 에 대한 인식이 부족하다. 그로 인해 실제 사용자는 다양한 보안 기능이 있음에도 설정 과정의 복잡함이나 부족한 기능 설명 등의 문제로 인해 적절하게 보안 기능을 사용하지 못하는 문제점이 있다. 이에 따라 본 논문에서는 Facebook의 보안 기능에 대한 사용자 편의성을 정량화 시킬 수 있는 방법을 제시하며, 실험을 통해 보안 기능 별 사용자 편의성에 대한 비교를 수행하였다.

ABSTRACT

Recently, as the widespread use of Facebook through a smartphone or tablet PC, it has increased the threat that contains the malicious code to post a social attacks and comments that use personal information that has been published of Facebook. To solve these problems, Facebook is, by providing a security function, but would like to address these threats, in setting the security function, the security function of the user's convenience is not considered a properly there is a problem that is not in use. Thus, in this paper, on the basis of the information obtained via the cogTool, on Facebook security features, the user experience by presenting a method that can be quantitatively measured by this, the user convenience It classifies about Facebook security features to decrease.

Keywords: Facebook, Usability, cogTool, Heuristic evaluation

I. 서 론

SNS(Social Network Service)는 최근 기존의 PC 뿐 아니라, 스마트 폰, 태블릿 PC와 같은 기기와 연동되어 사용이 점차 증가하고 있다. 사람들은 SNS을 통해 대인 관계를 형성하며, 정보의 공유, 감정의 표현과 같이 다양한 용도로 SNS를 이용하고 있다.

이러한 SNS는 사용용도, 기능, 목적에 따라 Facebook, Twiiter, Instram, Google Plus와 같은 다양한 서비스를 제공하고 있다. 특히 Facebook은 SNS 전체 사용자 중 약 80%의 점유율을 차지하고 있으며, 국내의 경우 약 1300만 명이 사용하는 가장 대중적인 SNS이다[13]. 이처럼 Facebook의 사용이 증가하고 기업들은 SNS로 획득한 대중들의 개인 취향 파악을 통해 마케팅에 이용

Received(12. 16. 2015), Modified(01. 26. 2016), Accepted(01. 26. 2016)
* 본 연구는 미래창조과학부 및 한국인터넷진흥원의 "2016년 고용계약형 정보보호 석사과정 지원사업"의 연구결과로 수행되었습니다.
† 주저자, 6sasimi@korea.ac.kr
‡ 교신저자, skim71@korea.ac.kr(Corresponding author)

하면서 상업적 중요성이 증가하고 있지만, 다양한 개인 정보가 Facebook에 노출됨에 따라 이를 악용하려는 움직임도 증가하고 있다. 실제 2010년에는 Facebook의 게시물과 채팅 메시지를 통해 악성코드가 유포된 일이 발생하기도 했다. 이와 같은 보안 위협에 대응하고자 Facebook에서는 보안 기능 및 보안 정책을 수립해 대응하고 있다. 하지만 Facebook의 자체적인 보안 기능 및 보안 정책이 있음에도 불구하고, 보안 기능을 설정하는데 있어 Usability 부족으로 사용자가 보안 기능을 적절히 사용하지 못하는 문제점이 발생하곤 한다. 따라서 본 연구에서는 Usable Security 관점에서 Facebook을 대상으로 보안 기능 설정의 Usability를 정량적으로 측정할 수 있는 방법을 제시하며, 이를 통해 보안 기능 설정 시 Usability 비교를 목표로 한다.

II. 관련 연구

2.1 Usability의 정의

ISO 9241-11에서 정의한 Usability란 사용자가 특정 제품 또는 특정 환경에서 목표를 달성하는 정도를 Usability라 하고 있으며, 이러한 정도의 측정 요소로는 Effectiveness, Efficiency, Satisfaction을 기준으로 하고 있다[1]. Effectiveness는 사용자가 목표로 한 Task를 달성할 수 있는가 여부 확인하는 요소이며, Efficiency는 이를 위해 소모한 자원을 의미한다. 또한 목표로 한 Task를 달성 시 소모한 자원, 시스템 절차와 같은 전반적인 과정의 만족 여부를 Satisfaction으로 정의한다[1]. 이러한 3가지 요소를 통해 Usability 평가 할 수 있다고 정의하였다. 하지만 기존의 보안 관련 솔루션은 Usability에 대한 인식이 부족해 보안 기능이 뛰어나더라도 사용이 어렵거나 설정 과정이 복잡해 사용되지 않는 경우가 다반사였다. 그렇기 때문에 보안 솔루션 사용에 있어 보안 기능 자체의 기능 뿐 아니라 사용자 관점에서 Usability 또한 충분히 고려되어야 한다.

2.2 GOMS 모델링

GOMS 모델링은 시뮬레이션을 통해 플랫폼, 기능 등의 Usability를 확인하는 모델링 기법이다.

GOMS 모델링은 인간과 컴퓨터의 상호작용을 하나의 문제해결행위로 보고 인간의 정보처리 과정에 대한 이론인 인지 복잡도 이론과 MHP(Model Human Process)에 근거한 실용적인 Usability 평가 방법이다. 또한 Fig.1과 같이 GOMS 모델링은 인간의 행위를 목표 (Goal), 조작(Operators), 방법(Methods), 선택규칙(Selection Rules)로 표현한다. 이러한 GOMS 모델링은 기본적으로 각 작업 목표에 정확한 수행단계를 정의하고 있으며, 사용자의 실수 및 시스템 상의 오류와 같은 사항은 고려하지 않는다는 가정을 하고 있다[2].

GOMS 모델링의 변형에는 KLM-GOMS (Keystroke-Level Model), CMN-GOMS (Card, Moran, and Newell-GOMS), CPM-

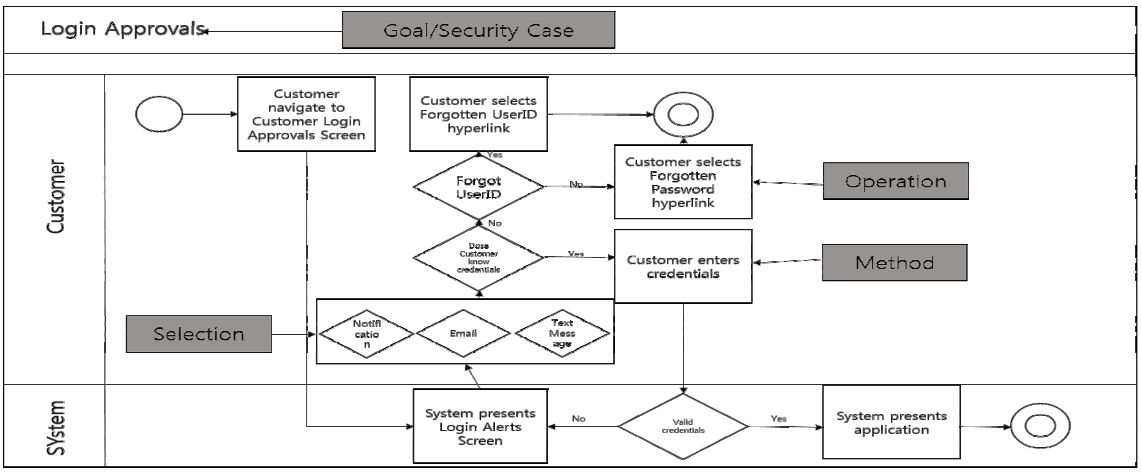

Fig. 1. GOMS modeling examples

GOMS (Cognitive Perceptual Motor GOMS & Critical Path Method GOMS), STM-GOMS (Security and Threat Model, Sensor-Touch-Mobile, Smart Technology Model)등이 있다[3][4].

이 중 KLM-GOMS는 가장 간단한 GOMS 방법으로 Task 수행을 위해 요구되는 기본적인 키와 마우스 입력의 총합을 예측하기 위한 방법이다.

이러한 KLM-GOMS을 통해 Task 수행을 측정하기 위한 Tool로는 cogTool이 있다. 본 논문에서는 cogTool를 통한 시뮬레이션을 통해 Usability을 측정한다[13].

2.3 Usability 평가 방법

기존의 Usability 평가 방법은 평가 주체에 따라 분류가 가능하다. Table 1.과 같이 평가 주체는 개발자, 평가자, 사용자가 있는데[7], 개발자는 소프트웨어 또는 시스템을 개발한 주체를 의미한다. 평가자는 일정 수준 이상의 경험과 전문 지식을 갖춘 대상을 의미하며, 이 밖에 경우에 해당하며 시스템을 사용하는 주체를 사용자로 분류할 수 있다. 이 중 Jakob Nielsen의 Heuristic Evaluation은 평가자들의 경험에 의한 직관적 사고를 바탕으로 평가하는 방법으로써 10개의 항목으로 정형화되어 있으며[6], 적은 수의 대상자를 통해서도 효율적인 결과를 도출할 수 있다는 장점이 있다. 설문조사에 경우 사용자의 만족도를 측정할 수 있다는 장점이 있다.

Table 1. Usability Evaluation methods

Center of Usability Evaluation	Method
Developer, Evaluator	Inspection in accordance with certain design guidelines
Evaluator	Heuristic Evaluation
	Cognitive Walkthrough
	Inspection in accordance with the general design guidelines
	Standard Inspection
User	Observation
	Questionnaire
	Affinity Diagram
Evaluator, User	Interview
	Contextual inquiry
Developer, Evaluator, User	Pluralistic walkthrough

본 논문에서는 이러한 평가 방법의 장점으로 체계화된 설문자료를 획득하기 위해 Heuristic Evaluation 기반의 체크리스트를 바탕으로 Satisfaction을 측정한다.

III. 연구 내용

3.1 Facebook에서 발생 가능한 보안 위협

유럽 ENISA(European Network and Information Security Agency)에서는 SNS 환경에서 발생 가능한 보안 위협을 4종류로 구분하고 이에 따른 세부 위협을 작성하였다[8]. Table 2.와 같이 ENISA에서 정의한 보안 위협에는 프라이버시 위협, 네트워크 보안 위협, ID 관련 인증 위협, 사회 공학적 위협이 있다. 프라이버시 위협은 SNS을 통해 노출되는 개인 프로필 정보 외에도 접속 위치, 이용 시간과 같은 추가적인 개인정보 획득을 통해 외부 공격자는 이를 활용한 해킹과 같은 공격에 이용할 수 있게 된다. 네트워크 보안 위협은 SNS의 게시물 혹은 댓글에 스팸 또는 바이러스가 포함되어 악용될

Table 2.Threats of SNS defined by ENISA

Threats	details
Privacy threats	Personal profile collection Secondary personal information (utilization time, the connection position) Weakening of anonymity associated with the development of face recognition technology Complete non-deletion of information on the SNS
Network Security Threats	SNS spam XSS, worms, viruses
ID management authentication threat	Phishing using SNS (EX: Spear Phishing) ID theft and deodorization
Social threats	Cyber Stalking Cyber Bullying Industrial espionage

수 있다. ID 관련 인증 위협의 경우 SNS를 이용한 피싱과 ID 도용과 위협이 존재하고 있다. 사회 공학적 위협은 SNS상에 드러나는 사진 혹은 연락처를 통해 사이버 스토킹과 같은 문제를 야기할 수 있다.

이러한 보안 위협 크게 2가지로 분류 가능하다. 하나는 Facebook 자체에 대한 보안 위협으로 서비스 제공자의 정책 변경 및 소프트웨어 개발을 통해 해결이 가능한 문제이다. 또 다른 보안 위협은 Facebook에서 제공하는 보안 기능을 통해 사용자가 감소시킬 수 있는 보안 위협이다. 본 논문에서는 2가지 보안 위협 중 사용자가 감소시킬 수 있는 보안 위협을 대상으로 하였다. 하지만 Facebook의 보안 기능에 분류가 되어 있더라도, SNS의 보안 위협에 대처하지 못하는 기능이 있으며 이와는 반대로 보안 기능으로 분류되어 있지 않음에도 보안 기능을 수행하는 기능 또한 존재한다. 따라서 본 논문에서는 기존의 Facebook의 설정 중 SNS 환경에서 발생 가능한 보안 위협을 예방할 수 있는 보안 기능을 연결 하였다.

Secondary data collection은 대상자의 이름 이외에도 연락처, Email, 이미지 업로드 시 위치 등을 외부 공격자가 획득 시 악용될 수 있는 보안 취약점이다[8]. 이러한 2차 정보의 노출을 방지하기 위해서 Facebook에서는 사용자가 업로드 한 게시물을 읽을 수 있는 대상을 지정하여 지정 대상 이외에는 현재 사용자의 접속 위치와 중요 게시물에 대한 접근을 차단할 수 있는데, 이러한 기능에는 Who can see my stuff, Who can contact me, Who can add things to my timeline, Who can see things on my timeline가 있다.

SNS spam은 사용자에게 광고성 글이나, 메시지를 보냄으로써 생기는 보안 취약점인데[8], 이를 방지하기 위해 댓글을 남길 수 있는 대상을 신뢰도가 높은 대상으로 제한할 수 있다. 또한 메시지를 통한 Spam의 경우도 메시지를 차단하는 기능을 통해 Spam 내용이 사용자에게 전달되는 것을 막을 수 있다. 이러한 기능은 Who can add things to my timeline, Block users을 통해 차단이 가능하다.

Cross Site Scripting, Viruses and Worms 취약점은 기본적으로 일반 사용자가 악의적인 URL로 접속을 해야 발생하는 취약점이다[8]. 이러한 보안 위협은 Who can add things to my timeline을 통해 악의적인 URL의 차단이 가능하다.

Cyber Stalking, Cyber Bullying, Industrial espionage 보안 위협은 일반 사용자의 게시물에 수치심을 느끼는 내용을 게시할 수 있는데[8], 이를 방지하기 위해서는 게시물에 댓글을 남길 수 있는 대상을 한정할 수 있다. Who can see things on my timeline, Who can add things to my timeline을 통해 대상에 대한 접근 권한을 제한할 수 있으며, Block users 등록을 통해 해당 사용자의 게시물 및 이벤트에 참여할 수 없게 수정이 가능하다.

ID theft and deodorization 보안 위협은 Facebook이 기존의 웹 이외에도 테블릿 PC, 스마트 폰과 같은 스마트 기기와의 연동이 보편화됨에 따라 계정에 대한 인증 과정에 있어 발생할 수 있는 보안 위협이다[8]. 이에 따라 Facebook에서는 인증과 관련된 보안 기능을 제공하고 있는데, 이러한 기능은 Login Alerts, Login Approvals, Trusted Contacts가 있다.

CBIR, Linkability from Image Metadata Tagging and Cross-profile Images 보안 위협은 Facebook에서 의도치 않은 사진이 태그 되거나 혹은 태그 된 이미지를 통해 외부 공격자가 2차적인

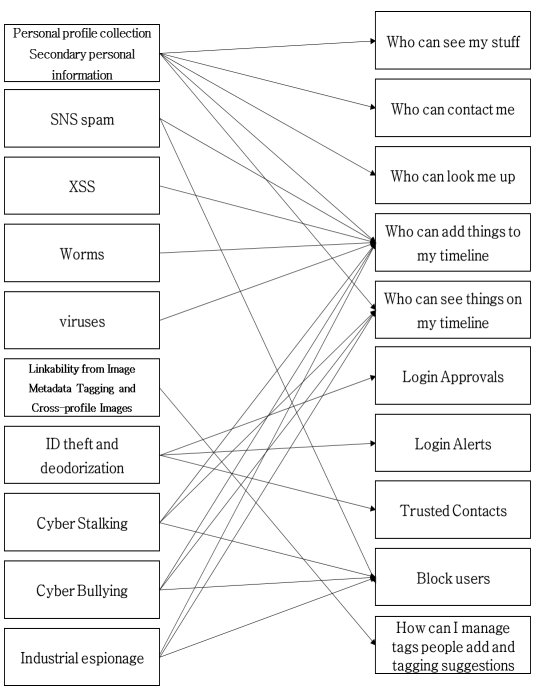

Fig. 2. Facebook security classification

피해를 발생시키는 보안 위협이다[8]. Facebook에서는 이미지 사진을 볼 수 있는 사람을 제한할 수 있으며, 사용자와 동일하게 인지된 사진에 대해서 공개, 비공개 여부를 설정할 수 있는데, How can I manage tags people add and tagging suggestions를 통해 이미지에 대한 접근 제한을 설정할 수 있다.

이와 같이 본 논문에서는 기존의 연구에서 분류된 보안 위협을 바탕으로[13] 현재 Facebook에서 제공하는 보안 기능을 통해 보안 기능과 보안 위협을 Fig 2.와 같이 맵핑시켰다.

3.2 cogTool

cogTool은 Carnegie Mellon 대학에서 개발한 Tool로써 KLM-GOMS 모델링을 적용한 시뮬레이션 Tool 이다. 일반적으로 cogTool은 숙련된 사용자를 대상으로 특정 Task 달성 시 소모된 총 시간 값을 측정하는 것이 주요 기능이다. 이러한 시간 값을 측정하기 위해 cogTool에서는 각각의 process를 시각화 시켜 나타낼 수 있다[9]. Fig. 3.은 cogTool을 이용한 시뮬레이션 결과이다[12].

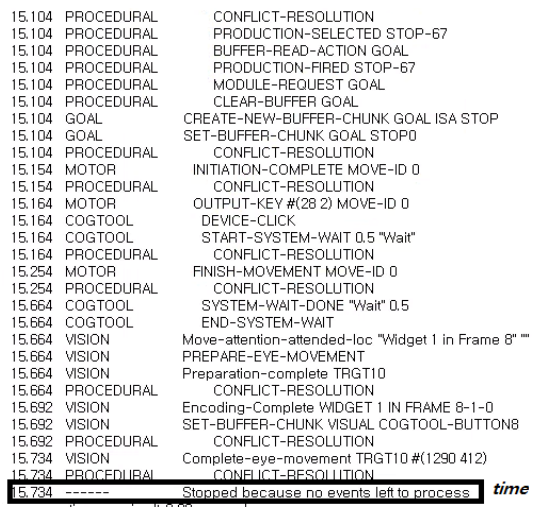

Fig. 3. simulation result

3.3 Usability 정량화

기존의 Usability 관련 연구에서는 Effectiveness, Efficiency, Satisfaction 각각의 요소를 개별적으로 판단하거나, 사용자 개인별 차이로 인해 정량화 시키지 못해 동일한 기능임에도 Usability를 객관적으로 측정하지 못하는 문제가 있었다. 본 논문에서는 Usability의 3가지 요소를 바탕으로 다음과 같은 수식을 통해 정량화 방법을 제안한다.

$$Usability = Effectiveness \times Efficiency \times Satisfaction$$

세부 항목의 상세 측정값은 다음과 같다.

3.3.1 Effectiveness

ISO 9241-11에서는 Effectiveness에 대한 정의를 사용자가 목표로 한 Task의 성공으로 정의하고 있다[1]. 하지만 이는 보안 관점에서 Effectiveness에는 해당하지 않는다. 따라서 본 논문에서는 보안 관정에서의 Effectiveness를 발생 가능한 보안 위협을 줄이는 것을 목표 Task로 설정하였다. Facebook에서 사용자가 설정 가능한 보안 기능은 Fig .2.와 같은데, 이러한 보안 기능에 각기 다른 중요도를 선정하였다. 예를 들어 자신의 타임라인에 댓글을 달 수 있는 대상을 제한하는 기능을 통해, 악의적인 3자에 의한 Spam 형식의 댓글 및 악성코드가 포함된 링크 제한 등의 총 8개의 보안 위협에 대응하는 설정이므로 중요도는 8이다. 또한, 보안 기능에는 각기 다른 공개 범위인 나만 보기, 친구만, 친구의 친구, 특정 대상, 모든 사람과 같이 5개의 경우가 있었는데, 이를 보안 기능의 설정 범위로 선정하였다. 나만 보기의 경우 Security 측면에서는 가장 높으므로 5로 설정하였고, 전체 공개는 상대적으로 Security가 낮으므로 1로 선정하였다. 이를 통해 Table 3.과 같은 보안 기능의 중요도와 공개 범위를 설정하였다.

Table 3. Importance and Coverage of security attributes

Security Attribute	importance	Coverage
Who can see my stuff?	1	Everyone(1)
		Friends of friends(2)
		Friends Only(3)
		Specific

		user(3)
		Myself(4)
Who can contact me?	1	Everyone(1)
		Friends of friends(2)
Who can look me up?	1	Everyone(1)
		Friends of friends(2)
		Friends Only(3)
Who can add things to my timeline?	8	Friends Only(3)
		Myself(4)
Who can see things on my timeline?	4	Everyone(1)
		Friends of friends(2)
		Friends Only(3)
		Specific user(3)
		Myself(4)
Login Alerts	1	It does not apply(1)
		Apply(2)
Login Approvals	1	It does not apply(1)
		Apply(2)
Trusted Contacts	4	It does not apply(1)
		Apply(2)
Block users	3	It does not apply(1)
		Apply(2)
Image Tag	1	Friends Only(3)
		Myself(4)

3.3.2 Efficiency

ISO 9241-11에서 정의한 Efficiency는 사용자가 보안기능을 변경하는데 소모한 자원을 의미한다[1]. 일반적으로 이러한 자원에는 시간, Error 횟수가 포함되지만, cogTool을 이용한 Efficiency 측정 방법에서는 Error 횟수는 예외처리가 된다. 따라서 본 논문에서는 Efficiency를 측정하기 위한 요소로 소모된 시간을 우선 측정한다. 또한 사용자가 보안 기능을 설정함에 있어 최종 goal을 달성하기 위한 절차가 복잡할 경우 소모 시간이 증가할 뿐 아니라, 버튼의 클릭 횟수도 증가하게 된다. 이는 사용자 측면에서 동일한 시간이 소모되더라도 Process step의 개수가 많은 경우 Efficiency가 떨어지게 된다. 따라서 본 논문에서는 Efficiency를 측정하기 위한 두 번째 요소로 Process step 개수를 측정하였다. 이러한 Process step 개수는 cogTool의 Visualization 기능을 활용할 경우 최종 목표를 달성하기 위한 전체 Process step 및 각각의 Process의 시간 값을 확인할 수 있다. cogTool에서 동일한 Process step 개수를 가지고 있음에도 실행시간이 다르게 나오는 것은 시뮬레이션 대상의 UI 및 button의 위치가 각기 달라 이를 인지하는데 걸린 시간이 다르기 때문이다. Fig. 4.는 cogTool를 이용해 보안 기능 설정 Process를 시각화 한 예시이다.

이와 같은 요소를 정의함으로써 본 논문에서는

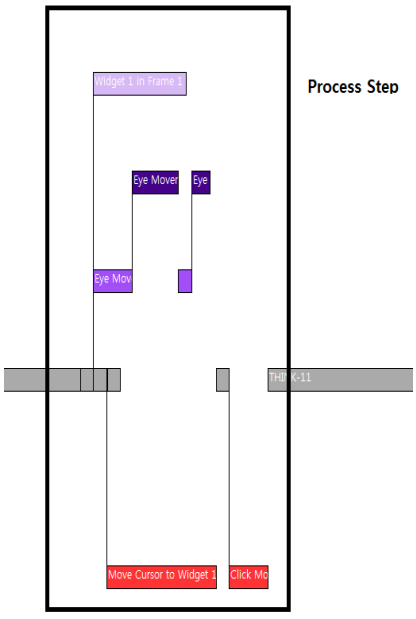

Fig. 4. cogtool simulation visualization

Table 4. Efficiency values

Efficiency	Value
	Time
	Step number

Efficiency를 측정하기 위한 요소를 Table 4.와 같이 설정하였다.

3.3.3 Satisfaction

Satisfaction은 기능 변경에 있어 절차, 시스템 상태의 시각화, 디자인, 도움말 제공과 같은 사용자별 만족도를 의미한다[1]. 이러한 만족도 측정을 위해 Jakob Nielsen이 제시한 Heuristic evaluation을 활용하였다. Heuristic evaluation은 10개의 주요 Category로 구성되어 있으며 평가 대상에 따라 세부항목이 유동적인데, Web Applications usability heuristic, Xerox 13 usability heuristic, Information Architecture heuristic, E-Commerce heuristic 등이 있다.

본 논문에서는 이러한 방법 중 Web Applications usability heuristic, Xerox 13 usability heuristic의 체크리스트를 활용하였다[10][11]. Web Applications usability heuristic은 웹 기반의 평가 대상인 경우에 적합한 방법이므로, Facebook에서 활용이 가능하다. 또한 Xerox 13 usability heuristic은 10개의 주요 Category에 대한 세부항목을 체크리스트로 만들었으며, 이러한 2개의 방법을 통해 Table 5.와 같은 세분화된 체크리스트를 구성하였다. 이후 Table 5.를 이용해 피실험자로 부터 각각의 항목에 SUS(System Usability Scale)를 1부터 5까지 입력받아 전체 항목에 대한 평균값을 구하여 Satisfaction을 정량화 한다.

Table 5. Heuristic evaluation Checklist

	Heuristic evaluation	Check List	SUS (1~5)
Satisfaction	Visibility of system status	It represents the state of the changed set values and system?	
	Match between system and the real world	Whether the description of the function is used familiar words, phrases, and concepts?	
	User control and freedom	It is possible again to undo the modified feature?	
	Consistency and standards	Whether the position is equal to the buttons on each page?	
		Terms of function has the consistency?	
	Error prevention	Whether there is ambiguous menus and commands to try to prevent user confusion and error?	
		To prevent mistakes by providing a predicted input value which is previously?	
		In order to avoid a fatal error, and offers a warning message at the time of the change of important information?	
	Recognition rather than recall	Did you express the setting value in a hierarchical structure?	
		It has been a clear visual division?	
	Flexibility and efficiency of use	In order to provide a variety of approaches, depending on the specialty, the shortcut is provided?	
		To provide a bunch function of the tasks that you frequently use?	

	Heuristic evaluation	Check List	SUS (1~5)
Satisfaction	Aesthetic and minimalist design	Is a simple UI design?	
		It offers a well-rounded picture of harmony?	
	Help users recognize, diagnose, and recover from errors	Warning messages are visually easily distinguished?	
		Whether the solution to the problem has been presented?	
		It was designed to allow error recovery?	
	Help and documentation	Help on the system, do you offer a manual?	
		Contents of help is not huge?	
		To provide to switch easily with help function?	

IV. 연구 결과

4.1 Facebook의 보안 기능 설정 시 Usability 측정

본 논문에서는 Facebook의 기능 중 보안 기능에 해당하는 10개의 기능을 분류하였다. 분류된 10개의 기능에 대해 Effectiveness, Efficiency, Satisfaction을 측정해 보안 기능 설정 시 Usability를 정량화 하였다.

4.1.1 Effectiveness 측정

본 논문에서는 Effectiveness를 측정하기 위해 보안 기능의 중요도 Importance (I)와 공개 범위 Coverage (C)를 통해 다음과 같은 수식을 정의한다.

$$Effectiveness\ Value(F) = Importance(I) + Coverage(C)$$

Effectiveness Value (F)의 값은 Table 3.을 기준으로 해당 실체 피험자들의 Facebook 계정에 설정되어 있는 공개 범위 및 설정 값을 측정하였다. 실제 피험자는 대학원생 12명을 대상으로 실험을 실시하였다. 해당 대상들의 평균 나이는 29.7세로 Facebook의 사용 기간은 평균 3.4년에 해당한다. 피실험자들은 남녀 각각 6명으로 구성되어 있다. 이를 통해 Effectiveness Value (F)을 측정한 결과 Table 6.과 같다.

4.1.2 Efficiency 측정

cogTool을 이용해 보안 기능 설정 시 소모된 시간과 step의 개수는 Table 7.와 같다. 또한 시간 값을 Time(T), Step 개수는 Step(S) 로 본 논문에서는 정의하였으며, Value(V)는 시간 값과 Step 개수의 곱으로 정의한다.

$$Value(V) = Time(T) \times Step(S)$$

Value(V)값은 시간 값과 Step의 개수에 따라 절대 값이 커지나. Efficiency value (E)는 시간 값

Table 6. Effectiveness of security attributes

Security Attribute	Average Effectiveness
Who can see my stuff?	4.75
Who can contact me?	2.75
Who can look me up?	4.25
Who can add things to my timeline?	8
Who can see things on my timeline?	6.5
Login Alerts	2.25
Login Approvals	2
Trusted Contacts	1.125
Block users	1
Image Tag	2

Table 7. Time Value, Step of security function

Category	Security Attribute	Time(T)	Step(S)	Efficiency Value(E)
Privacy Settings and Tools	Who can see my stuff?	15.7	8	0.8
	Who can contact me?	10.5	5	2.2
	Who can look me up?	9.6	5	2.1
Timeline and Tagging Settings	Who can add things to my timeline?	9.7	5	2.1
	Who can see things on my timeline?	11.4	6	1.5
Security Settings	Login Alerts	15.4	6	1
	Login Approvals	22.5	9	0.4
	Trusted Contacts	16.2	6	1
	Image Tag	15.8	6	1.1
Manage Blocking	Block users	8.2	3	4

과 Step의 개수가 적을수록 값이 커지므로 Value(V) 값과 Efficiency value (E)는 반비례 관계에 있다.

$$Efficiency\ Value(E) = \frac{1}{Value(V)} \times 100$$

이와 같은 식을 적용 시 Table 7.의 결과와 같이 분류된 10개의 Facebook 보안 기능 중 불필요한 사용자를 차단하는 기능의 경우 시뮬레이션 결과 가장 적은 시간이 소요되고, Step 개수가 가장 적었으며 Efficiency Value (E) 값이 4로 가장 크게 도출되었다. 반면에 로그인 승인의 경우 소요되는 시간과 Step의 개수가 가장 많았으며 Efficiency Value (E) 값이 0.4로 가장 작은 결과가 도출되었다.

4.1.3 Satisfaction 측정

Facebook 보안 기능 설정에 있어 Satisfaction을 측정하기 위해 대학원생 12명을 대상으로 실험을 실시하였다. 해당 대상들의 평균 나이는 29.7세로 Facebook의 사용 기간은 평균 3.4년에 해당한다. 피실험자들은 남녀 각각 6명으로 구성되어 있다. 피실험자들을 대상으로 분류된 보안 기능 9개에 대해 Table 5. Heuristic evaluation 체크리스트를 통해 Satisfaction을 측정하였다. Satisfaction값의 범위는 1~5사이이다. Table 8. 각 보안 기능 설정에 대한 Satisfaction을 나타낸다.

Table 8. Satisfaction of security attributes

Security Attribute	Average Satisfaction
Who can see my stuff?	2.8
Who can contact me?	3.7
Who can look me up?	3.7
Who can add things to my timeline?	3.7
Who can see things on my timeline?	3.5
Login Alerts	4.0
Login Approvals	2.2
Trusted Contacts	4.0
Block users	4.6
Image Tag	3.5

4.1.4 Usability 분석 및 실험 결과 비교

보안 기능 별 Effectiveness 분류를 Effectiveness Value (F)와 cogTool을 통해 획득한 Efficiency value (E) 값과 Heuristic evaluation 체크리스트를 통해 추출한 Average Satisfaction으로 Usability를 구하면 Fig. 5와 같다. 실험을 통해 사용자에게 댓글을 남기는 기능의

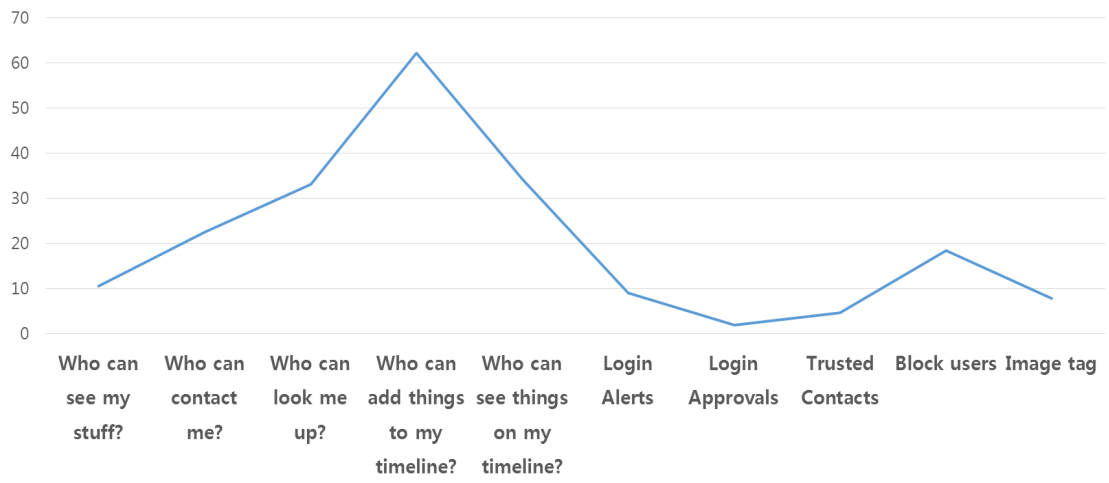

Fig. 5. Facebook usability of security features

경우 해당 대상을 통해 다양한 보안위협에 대처가 가능할 뿐 아니라, Efficiency value (E) 값과 Average Satisfaction 값이 상대적으로 높게 측정이 되었다. 반면 다른 기기를 통한 로그인 승인의 경우는 보안코드 생성과 같은 세부절차가 복잡해 Efficiency value (E) 값과 Average Satisfaction이 떨어져 Usability가 가장 낮게 측정되었다.

V. 결론 및 향후 과제

본 연구에서는 Facebook에서 제공하는 설정 중 보안 기능을 분류하였으며, 이를 토대로 보안 기능 설정 절차에 있어 Usability를 정량화 시킬 수 있는 방법을 제안하였다. 제안한 방법을 통해 실험을 진행한 결과 상대적으로 Effectiveness와 Efficiency가 떨어지는 기능과 설정 절차가 복잡해 사용자 Satisfaction이 떨어지는 보안 기능이 존재하고 있었다.

향후에는 본 논문에서 제시한 보안 기능에 대한 Usability 개선 방안에 대해 연구하고, Effectiveness와 Satisfaction 확인을 위한 실험의 경우 대상이 대학원생에 한정되어 있는 점을 개선하여 다양한 실험 대상을 선정하여 연구 범위를 확대할 예정이다.

References

[1] Jokela, Timo, et al, "The standard of user-centered design and the standard definition of usability: analyzing ISO 13407 against ISO 9241-11," Proceedings of the Latin American conference on Human-computer interaction. ACM,pp. 53-60. Aug. 2003.

[2] Din, Amran, "Usable Security using GOMS: A Study to Evaluate and Compare the Usability of User Accounts on E-Government Websites," Nova Southeastern university. 2015.

[3] Shin, Sooyeon, and Taekyoung Kwon, "STM-GOMS Model: A Security Model for Authentication Schemes in Mobile Smart Device Environments," Journal of the Korea Institute of Information Security and Cryptology 22(6). pp. 1243-1252. 2012.

[4] Card, Stuart K. Thomas P. Moran, and Allen Newell, "The keystroke-level model for user performance time with interactive systems," Communications of the ACM vol. 23. no. 7 pp.396-410. 1980.

[5] Bellamy, Rachel, et al, "Using CogTool to model programming tasks,"

Evaluation and Usability of Programming Languages and Tools. ACM, Oct. 2010.
〔6〕 Nielsen Jakob, "Usability engineering," Elsevier, pp. 1-362. Oct. 1994.
〔7〕 Nielsen Jakob, "Usability inspection methods," Conference companion on Human factors in computing systems. ACM, pp. 413-414. Apr. 1994.
〔8〕 Giles Hogben, "security issues and recommendations for online social networks," ENISA Position Paper No.1, pp. 1-36. Oct. 2007.
〔9〕 Bellamy, Rachel, Bonnie John, and Sandra Kogan, "Deploying CogTool: integrating quantitative usability assessment into real-world software development," Software Engineering (ICSE), 2011 33rd International Conference on. IEEE, pp. 691-700. May. 2011.
〔10〕 jordisan, "Web Applications (RIA) usability heuristics," http://ucdmanager.net/heuristics/web-applications-ria-usability-heuristics.
〔11〕 Deniese Pierotti at Xerox Corporation, "Xerox 13 usability heuristics," http://ucdmanager.net/heuristics/xerox-13-usability-heuristics.
〔12〕 "cogtool tutorial," https://github.com/cogtool/documentation/tree/master/end-user/tutorial.
〔13〕 Hyeob Kim, "Factors Affecting Intention to Use Security Functions in SNS," Korea Society of IT Service Journal 13(2). pp. 1-17. Jul. 2014.

〈저자소개〉

김 청 한 (Chung-han Kim) 학생회원
2013년 8월: 광운대학교 컴퓨터소프트웨어학과 졸업
2014년 3월~현재: 고려대학교 정보보호대학원 금융보안학과 석사과정
〈관심분야〉 정보보증, 정보보호관리체계, Usable Security

박 민 수 (Min-su Park) 학생회원
2010년 2월: 신라대학교 컴퓨터네트워크학과 졸업
2013년 2월: 고려대학교 정보보호대학원 정보보호학과 석사
2013년 3월~현재: 고려대학교 정보보호대학원 정보보호학과 박사과정
〈관심분야〉 정보보증, 정보보호제품 보안성 평가, 디지털 포렌식, Usable Security

김 승 주 (Seung-joo Kim) 종신회원
1994년~1999년: 성균관대학교 정보공학과 (학사, 석사, 박사)
1998년 12월~2004년 2월: KISA(舊한국정보보호진흥원) 팀장
2002년~현재: 한국정보통신기술협회(TTA) IT 국제표준화전문가
2004년 3월~2011년 2월: 성균관대학교 정보통신공학부 조교수, 부교수
2011년 3월~현재: 고려대학교 사이버국방학과/정보보호대학원 정교수
2004년~현재: 한국정보보호학회 이사
2005년~2006년: 교육인적자원부 유해정보 차단 자문위원
2007년: 국가정보원장 국가사이버안전업무 유공자 표창
2007년~2009년: 전자 정부 서비스 보안 위원회 사이버 침해사고대응 실무위원회 위원
2010년: 방송통신위원회 정보통신망 침해사고 민관합동조사단 위원
2012년 3월~2012년 6월: 선관위 디도스 특별검사팀 자문위원
2013년 4월~2013년 12월: IT보안인증사무국 자문위원
2013년 9월~현재: 중앙선거관리위원회 자문위원
2014년 3월~현재: 헌법재판소 자문위원
2014년 12월~현재: 카카오 자문위원
2016년 1월~현재: 한국정보화진흥원 자문위원
〈관심분야〉 보안공학, 암호이론, 정보보증, 정보보호제품 보안성 평가, Usable Security